[DvSPAM]

SPAM-Filter für Tobit® David®
Version 6.2

SyntaX Software Wismar 2015

1 Lizenzbedingungen 1

2 Grundlagen 3

2.1 Die Key-Features von DvSPAM 3
2.2 DvSPAM im Überblick 4
2.3 Komponenten 5
2.4 Einschränkungen der Demo-Versionen 6

3 Systemvoraussetzungen 7

4 Installation 8

4.1 Installationsvarianten 8
4.2 Vorbereitung der Installation bei David unter Windows 8
4.3 Vorbereitung der Installation bei David unter Netware 11
4.4 Vorbereitung der Installation bei David unter Linux 14
4.5 Installation 14

5 Konfiguration 17

5.1 Registerkarte Archivauswahl 17
5.2 Registerkarte Spam Konfiguration 20
5.3 Registerkarte Black/Whitelisten 25
5.4 Registerkarte DNS Blacklisten 27
5.5 Registerkarte automatische Whitelist 28
5.6 Registerkarte Schlüsselwörter 29
5.7 Registerkarte Spamwertung 30
5.8 Registerkarte Benachrichtigungen 32
5.9 Registerkarte Service 33
5.10 Registerkarte Monitor 35
5.11 Info/Lizenzierung Button 36
5.12 Linux-spezifische Konfiguration 38

6 Anhang 39

6.1 Support / Kontakt 39

1 Lizenzbedingungen

Indem der Lizenznehmer das SOFTWAREPRODUKT installiert, kopiert oder anderweitig verwendet oder gebraucht, erklärt er sein Einverständnis mit diesen LIZENZBEDINGUNGEN der SyntaX Software. Falls der Lizenznehmer diesen Bestimmungen nicht zustimmt, ist er nicht berechtigt, das SOFTWAREPRODUKT zu installieren und/oder in einer anderen Form zu verwenden.

SyntaX Software behält sich sämtliche Eigentums- und Schutzrechte, insbesondere alle Urheber-, Patent- und Markenrechte sowie Geschäftsgeheimnisse und sonstige Schutzrechte an dem SOFTWAREPRODUKT vor, einschließlich, aber nicht beschränkt auf Bilder, Fotografien, Animationen, Video, Audio, Musik, Text und "Applets", die in dem SOFTWAREPRODUKT enthalten sind, den gedruckten Begleitmaterialien und jeder Kopie des SOFTWAREPRODUKTS. Der Lizenznehmer ist nicht berechtigt, die SOFTWARE vollständig oder teilweise zu verändern oder daraus abgeleitete Produkte anzufertigen. Der Lizenznehmer darf keine Urheberrechtshinweise, sonstige Eigentumsrechtshinweise oder Etiketten von den Produkten entfernen.
Aus diesem Grund ist der Lizenznehmer verpflichtet, das SOFTWAREPRODUKT wie jedes andere durch das Urheberrecht geschützte Material zu behandeln, mit der Ausnahme, dass er berechtigt ist, das SOFTWAREPRODUKT zur Archivierung eines einzigen Servers zu installieren. Der Lizenznehmer ist berechtigt, den originalen Datenträger zu kopieren, vorausgesetzt, er bewahrt das Original ausschließlich für Sicherungs- und Archivierungszwecke auf. Der Lizenznehmer ist nicht berechtigt, die das SOFTWAREPRODUKT begleitenden gedruckten Materialien zu vervielfältigen.

Der Lizenznehmer ist nicht berechtigt, das SOFTWAREPRODUKT zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung dies ausdrücklich gestattet. Der Lizenznehmer ist nicht berechtigt, das SOFTWAREPRODUKT zu vermieten, zu verleasen oder zu verleihen.

SyntaX Software bietet dem Lizenznehmer möglicherweise Supportleistungen in Verbindung mit dem SOFTWAREPRODUKT ("Supportleistungen"). Die Supportleistungen können entsprechend den Bestimmungen, die im Benutzerhandbuch, der Dokumentation im "Online"-Format und/oder anderen von SyntaX Software zur Verfügung gestellten Materialien beschrieben sind, genutzt werden. SyntaX Software ist berechtigt, die technischen Daten, die der Lizenznehmer SyntaX Software als Teil der Supportleistungen zur Verfügung stellt, für geschäftliche Zwecke, einschließlich der Produktunterstützung und -entwicklung, zu verwenden. SyntaX Software verpflichtet sich, solche technischen Daten ausschließlich anonym im Sinne des Datenschutzes zu verwenden.

Haftung:
ÜBER DIE HIER ANGEGEBENEN GEWÄHRLEISTUNGEN HINAUS, ÜBERNIMMT SYNTAX SOFTWARE KEINE WEITERGEHENDE GEWÄHRLEISTUNG FÜR SYNTAX SOFTWARE PRODUKTE. DIE AUSWAHL, INSTALLATION, UND VERWENDUNG DER FÜR DIE VORGESEHENEN ZWECKE GEEIGNETEN SOFTWARE UND DAS ERZIELEN DER GEWÜNSCHTEN ERGEBNISSE LIEGEN ALLEIN IN DER VERANTWORTUNG DES LIZENZNEHMERS. IN DEN BEGLEIT-MATERIALIEN (DOKUMENTATIONEN etc.) ENTHALTENE SPEZIFIKATIONEN UND LEISTUNGSMERKMALE STELLEN AUSDRÜCKLICH KEINE IM SINNE VON § 463 BGB ZUGESICHERTE EIGENSCHAFT DAR, SOFERN SIE NICHT AUSDRÜCKLICH VON SYNTAX SOFTWARE ALS SOLCHE BEZEICHNET WERDEN.

Das SOFTWAREPRODUKT und die dazugehörige Dokumentation wird wie angegeben zur Verfügung gestellt, ohne jede Gewährleistung oder Bedingungen jeglicher Art, sei sie ausdrücklich oder konkludent, einschließlich, jedoch nicht beschränkt auf, jeder konkludenten Gewährleistung und Bedingung im Hinblick auf Handelsüblichkeit, Eignung für einen bestimmten Zweck oder Nichtverletzung von Rechten Dritter. Das gesamte Risiko, das bei der Verwendung oder Leistung des SOFTWAREPRODUKTS entsteht, verbleibt beim Lizenznehmer.

Soweit gesetzlich zulässig, sind SyntaX Software oder deren Lieferanten in keinem Fall haftbar für irgendwelche Folge-, zufälligen, direkten, indirekten, speziellen, strafrechtlichen oder anderen Schäden welcher Art auch immer (einschließlich, aber nicht beschränkt auf Schäden für entgangenen Gewinn, Geschäftsunterbrechung, Verlust von geschäftlichen Informationen oder andere Vermögensschäden), die aus diesem Vertrag oder der Verwendung des SOFTWAREPRODUKTS oder der Tatsache, dass es nicht verwendet werden kann, resultieren, selbst wenn SyntaX Software auf die Möglichkeit solcher Schäden hingewiesen worden ist.
Darüber hinaus haftet SyntaX Software für entstandene Schäden nur insoweit, als SyntaX Software Vorsatz oder grobe Fahrlässigkeit zur Last fällt. Weiterhin haftet SyntaX Software bis zur Höhe des typischerweise voraussehbaren Schadens auch für solche Schäden, die SyntaX Software oder Ihren Erfüllungsgehilfen in Verletzung einer wesentlichen Vertragspflicht verursacht haben.
Der Lizenznehmer ist verpflichtet, in angemessenen Abständen, jedoch mindestens einmal am Tag, Sicherungskopien seiner sämtlichen Daten anzufertigen. Eine Verletzung dieser Pflicht gilt als erhebliches Mitverschulden.

SyntaX Softwares gesamte Haftung ist beschränkt auf den höheren der beiden Beträge für den tatsächlich für das SOFTWAREPRODUKT gezahlten Preis oder € 100,-. Die Vereinbarung dieser Haftungshöchstgrenze ist für SyntaX Software Grundvoraussetzung für den Abschluss dieses Vertrages.

Diese Haftungsbegrenzung gilt im Hinblick auf alle Schadensersatzansprüche, unabhängig von ihrem Rechtsgrund, insbesondere auch im Hinblick auf vorvertragliche und nebenvertragliche Ansprüche. Die Haftungsbeschränkung schränkt eine gesetzliche zwingende Haftung nach dem Produkthaftungsgesetz oder eine Haftung für zugesicherte Eigenschaften nicht ein, soweit die zugesicherte Eigenschaft den Lizenznehmer gerade vor dem eingetretenen Schaden schützen sollte.

Salvatorische Klausel:
Sollten einzelne Bestimmungen dieser Lizenzbedingungen unwirksam oder nichtig sein oder werden, so berührt dies die Gültigkeit der übrigen Lizenzbedingungen nicht.

Zusätzliche Bedingungen für die Software DvSPAM:
DvSPAM klassifiziert eingehende Emails nach bestimmten Gesichtspunkten als erwünscht oder unerwünscht. Diese Kriterien werden teilweise vom Anwender konfiguriert und sind teilweise durch die Architektur der Software vorgegeben. Die Hauptfunktion dieser Software besteht darin, den Großteil unerwünschter Emails vom Anwender fern zu halten. SyntaX Software haftet auf keinen Fall und insbesondere nicht für Schäden aller Art, die durch eine vom Anwender unerwartete Klassifizierung und eine dadurch eventuell unerwartete Verteilung von Emails entstanden sind.

2 Grundlagen

Vielen Dank, dass Sie sich für DvSPAM entschieden haben.

DvSPAM dient der automatischen Filterung von SPAM-Nachrichten aus den Archiven von Tobit David©.

DvSPAM bildet eine in David integrierte Schnittstelle zu dem universell einsetzbaren Mailfilter procmail und dem in diesem System als „Procmail-Skript“ laufenden SPAM Filter NiXSpam der Zeitschrift iX des Heise Verlages.

Dieses Procmail-Skript ist auf großen Durchsatz ausgelegt und treibt einigen Aufwand (Prüfsummen, Whitelist, Blacklist), der dafür sorgt, dass nur ein Bruchteil aller Mails die CPU-belastende Inhaltsanalyse durchlaufen muss. Außerdem sind wichtige Informationen über laufende Spam-Attacken schnell von den Web-Seiten des Heise-Verlags via Internet verfügbar. NiX Spam testet besonders die Received:-Header-Zeilen intensiv und beurteilt die (nicht durch Checksum bekannten) E-Mails schon nach der Header- und MIME-Analyse und lässt die rechenintensive Body-Analyse bei eindeutiger Lage (also meistens) aus. Es gibt daher keine Schlussbewertung auf einer kontinuierlichen Skala, sondern eines der folgenden Resultate: HAM, MAYBESPAM, SPAM, WHITE oder BLACK. WHITE oder BLACK geben an, ob die jeweilige Email-Adresse in der White- bzw. Blackliste enthalten ist.

Zu den Details dieses Filters kann auf die beiden iX Artikel aus den Ausgaben 05/2003 und 11/2003 verwiesen werden. Notwendige Filterinformationen werden vom Verlag kostenlos zur Verfügung gestellt und mehrfach täglich aktualisiert.

Vor der Bewertung durch das Procmail-Skript werden als David-Archiv implementierte White und Black List zur Bewertung der eingehenden Emails herangezogen. Zusätzlich ist es möglich, David Adress-Archive als White Lists zu verwenden.

DvSPAM integriert diese Bewertung durch konfigurierbare Aktionen nahtlos in Tobit David.

2.1 Die Key-Features von DvSPAM

DvSPAM bietet folgende Vorteile:

- DvSPAM **kostet nur einmal Geld**: DvSPAM wird einmalig als Lizenz erworben. Die laufenden Aktualisierungen von DvSPAM über das Internet sind kostenfrei.
- DvSPAM ist **selbst lernend**: Alle Email-Adressen, an die Sie Emails senden, werden durch DvSPAM in einer automatischen White List geführt. So werden die Emails Ihrer Geschäftspartner garantiert nicht als SPAM klassifiziert.
- DvSPAM unterstützt neben der **automatischen White List** auch eine **globale manuelle White List** sowie eine **globale manuelle Black List**. Die manuellen Listen sind als **David-Archive** implementiert.
- Außerdem können für jeden David User **persönliche White- und Blacklisten** verwendet werden. Auch diese sind als **David-Archive** implementiert.
- DvSPAM unterstützt die Abfrage von DNS Blacklisten.
- DvSPAM kann beliebige David **Adress-Archive** als **Whitelist** verwenden.
- DvSPAM unterstützt **David ab der Version 6.6** unter Windows, Netware und Linux.
- Eventuell beim Provider bereits vorhandene Vorsatzfilter werden optional bei der Klassifizierung berücksichtigt.
- Das resultierende Ergebnis der Klassifizierung wird optional in den Kommentar der Nachrichten geschrieben und kann so vom Empfänger im David Client eingesehen werden.

2.2 DvSPAM im Überblick

DvSPAM enthält die folgenden Filterfunktionen, die in der genannten Reihenfolge abgearbeitet werden. Liefert ein Filter ein Ergebnis wird die Abarbeitung abgebrochen.

Manuelle Whitelist + Adress-Archive:

- Alle eingehenden Nachrichten mit Absenderadressen aus dieser Liste werden als erwünschte Mail (WHITE) behandelt.
- die Liste kann enthalten:
    - Nachrichten mit kompletten Emailadressen
      Zum Hinzufügen wird eine empfangene Mail von dem gewünschten Absender in dieses Verzeichnis kopiert oder verschoben. Nicht benötigte Informationen dieser kopierten Mail werden von DvSPAM automatisch gelöscht, so dass nur noch die Absenderadresse übrig bleibt.
    - Adresseinträge mit kompletten Emailadressen oder nur mit dem Domainname.
      In der manuellen Whitelist kann ein David Adresseintrag angelegt, in dieses Archive kopiert oder verlinkt werden. Dieser kann im Feld eMail eine komplette Mailadresse (test@firma.de) oder nur einen Domainnamen (@firma.de) enthalten. Wird nur der Domainname eingetragen, werden alle Mails dieser Domain als WHITE klassifiziert.

Manuelle Blacklist:

- Alle Nachrichten mit Absenderadressen aus dieser Liste werden als unerwünschte Mail (BLACK) behandelt.
- die Liste kann enthalten:
    - Nachrichten mit kompletten Emailadressen
      Zum Hinzufügen wird eine empfangene Mail von dem unerwünschten Absender in dieses Verzeichnis kopiert oder verschoben. Nicht benötigte Informationen dieser kopierten Mail werden von DvSPAM automatisch gelöscht, so dass nur noch die Absenderadresse übrig bleibt.
    - Adresseinträge mit kompletten Emailadressen oder nur mit dem Domainname.
      In der manuellen Blacklist kann ein David Adresseintrag angelegt, in dieses Archive kopiert oder verlinkt werden. Dieser kann im Feld eMail eine komplette Mailadresse (test@firma.de) oder nur einen Domainnamen (@firma.de) enthalten. Wird nur der Domainname eingetragen, werden alle Mails dieser Domain als BLACK klassifiziert.

Automatische Whitelist:

- Alle eingehenden Nachrichten mit Absenderadressen aus dieser Liste werden als erwünschte Mail (WHITE) behandelt.
- In diese Liste nimmt DvSPAM automatisch alle Email Adressen auf, an die David Benutzer eine Nachricht senden. So werden Nachrichten von Kunden und Geschäftspartnern unabhängig vom Inhalt garantiert nicht als SPAM klassifiziert! Interne Mails und Empfänger mit eigener Domain werden nicht in die Liste eingetragen.
- Diese Liste wird im DvSPAMadministrator angezeigt und kann dort bearbeitet werden.

Alias Überprüfung:

- Wird eine Mail mit einem Empfänger empfangen, der nicht in der Aliasliste enthalten ist, wird diese Mail als SPAM gekennzeichnet. Diese Funktion muss im DvSPAMadministrator aktiviert werden.

DNSBL:

- DvSPAM kann DNS Blacklisten abfragen. Per Default sind 3 verschiedene Listen eingetragen. Diese können auf Wunsch geändert oder weitere zusätzlich eingetragen werden.
- als Ergebnis sind HAM bzw. SPAM möglich

NiXSpam Filter:

- der NiXSpam Filter ist ein procmail Skript, vorgestellt in den Ausgaben 05/2003 und 11/2003 der Zeitschrift iX und seit dem mehrfach verbessert.
- zur Funktionsweise siehe die beiden oben genannten Artikel
- als Ergebnis liefert das Skript drei verschiedene Wertungen: HAM, MAYBESPAM und SPAM

Der ursprüngliche NiXSpam Filter wurde dahingehend modifiziert, dass eine David-konforme Behandlung durch DvSPAM möglich ist.

Auswirkung der Klassifizierung:

Wurde eine Mail als SPAM/BLACK oder MAYBESPAM klassifiziert, werden die im DvSPAMadministrator konfigurierten Aktionen durchgeführt. Folgende Aktionen sind dabei möglich:

- Markieren der Nachricht mit einem David-Flag
- Ändern der Farbe der Nachricht
- Ändern des Betrefftextes
- Kopieren der Nachricht in ein anderes Archiv
- Verschieben der Nachricht in ein anderes Archiv

Eine als HAM/WHITE klassifizierte Nachricht wird nicht modifiziert.

Das Ergebnis der Klassifizierung der Nachrichten kann optional in der Kommentardatei der jeweiligen Nachricht hinterlegt und so vom Empfänger im David Client eingesehen werden. Das Ergebnis der Klassifizierung wird ebenfalls in die Spalte *Identifizierung* im David Client eingetragen.
Eine weitere Option ist die Berücksichtigung der Bewertung eventuell vorgesetzter Mailfilter. Es können Ergänzungen der Betreff-Zeile oder des Mailheaders berücksichtigt werden. Näheres zu diesem Thema finden Sie im Kapitel 5.3.

2.3 Komponenten

DvSPAM besteht aus den Komponenten DvSPAMservice, DvSPAMadministrator, und DvSPAMcheck.

Der **DvSPAMservice** übernimmt die automatische Klassifizierung der Nachrichten und führt die konfigurierten Aktionen durch.

Der **DvSPAMadministrator** dient der Konfiguration und Überwachung des DvSPAMservice. Im DvSPAMadministrator werden unter anderem die erforderlichen Pfade, die NiXSpam Konfiguration und die zu berücksichtigenden Eingangsarchive mit den dazugehörigen Aktionen konfiguriert. Die Lizenzierung erfolgt ebenfalls über den DvSPAMadministrator.

DvSPAMcheck ist eine Erweiterung für den David Client auf dem DvSPAM Administrations-PC und dient der Überprüfung der Filterfunktionen. Die Applikation wird über das Kontextmenü einer Nachricht aufgerufen und zeigt die Ausgaben der Filter mit der aktuellen Konfiguration und die Original-Nachricht an. Damit können Änderungen der DvSPAM Konfiguration sofort getestet werden. Für die Interpretation der Ausgaben des NiXSpam Filters wird wiederum auf die Ausgaben 05/2003 und 11/2003 der Zeitschrift iX verwiesen.

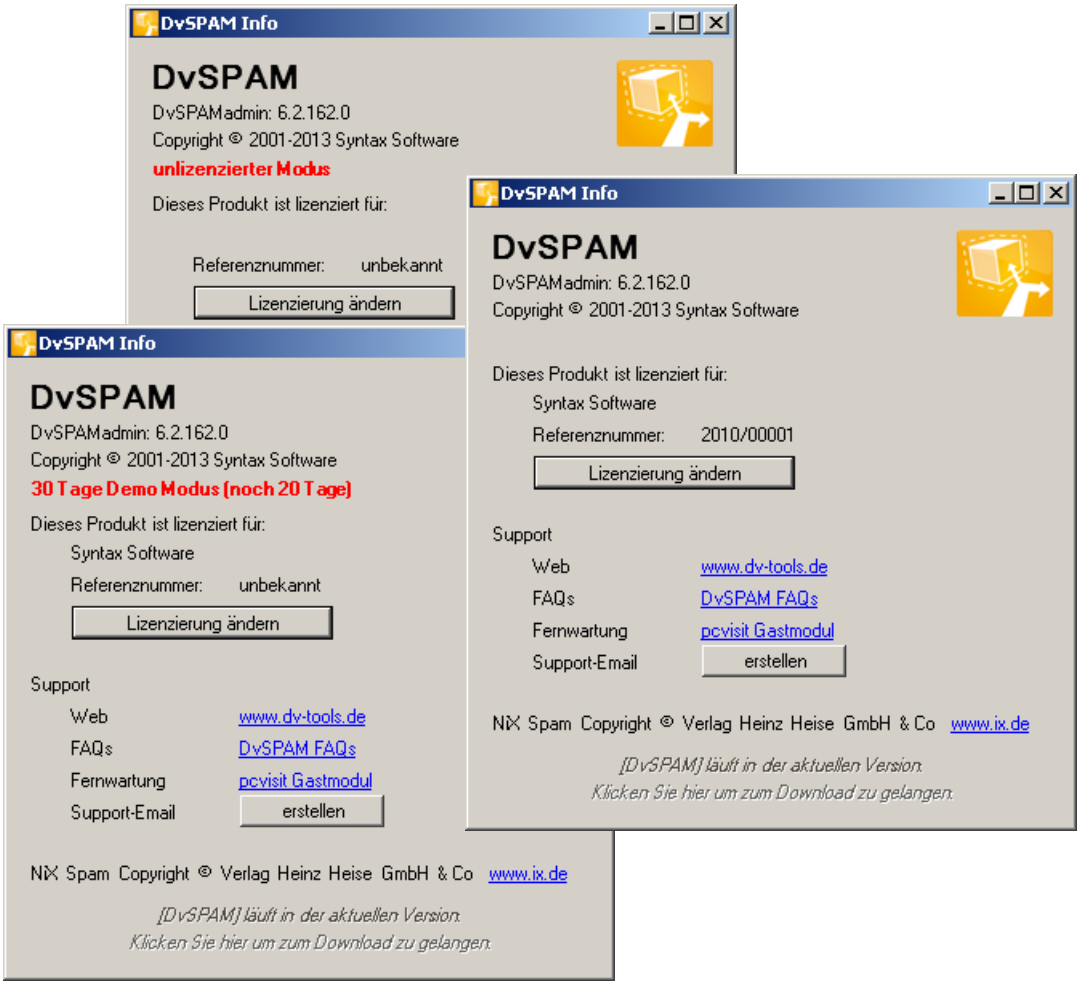
2.4 Einschränkungen der Demo-Versionen

DvSPAM unterscheidet drei unterschiedliche Modi: den unlizenzierten, den 30 Tage Demo und den lizenzierten Modus.

Im unlizenzierten Modus von DvSPAM ist es möglich, alle Funktionen vom DvSPAMadministrator und von DvSPAMcheck zu nutzen. Es ist aber nicht möglich, den DvSPAM Service zu starten.

Für den 30 Tage Demo-Modus von DvSPAM fordern Sie bitte im Fenster Info/Lizenzierung eine Demo Lizenz an. Sie erhalten diese per Mail und können mit ihr 30 Tage den gesamten Funktionsumfang von DvSPAM testen. Nach Ablauf dieser Frist schaltet DvSPAM in den unlizenzierten Modus.

Soll nach dem Test von DvSPAM eine Vollversion eingesetzt werden, ist die Lizenzdatei *lizenz.xml* auszutauschen, die Konfiguration gegebenenfalls zu vervollständigen und der DvSPAM Service neu zu starten.



3 Systemvoraussetzungen

Generell gelten die gleichen Systemvoraussetzungen wie für David unter Windows. Zusätzlich sind folgende Voraussetzungen zu beachten:

Hauptspeicher	mindestens 512 Mbyte
Plattenspeicher für DvSPAM	ca. 50 Mbyte
Betriebssysteme	Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2012 (32- und 64-bit)
.NET Framework v2.0	.NET Framework Version 2.0 Redistributable Package erforderlich .NET Framework SDK Version 2.0 alternativ möglich Bei der Installation kann das Framework über das Internet mit installiert werden. Alternativ finden Sie einen Link zur benötigten Version im DvSPAM Download Bereich unter www.dv-tools.de.
David	Windows, Netware oder Linux Support für David ab Version 10 zusätzlich wird auf dem DvSpam Service PC ein David Client benötigt

4 Installation

4.1 Installationsvarianten

DvSPAM unterstützt David Installationen ab 6.6 SP6a unter Windows ab der Version 2000, unter Netware ab Version 4 und unter Linux. Dabei kann DvSPAM auf dem David-Server (empfohlen) oder auf einem anderen Server oder einer Workstation installiert werden. **DvSPAM ist ein Windows-Programm und muss deshalb bei einer David-Installation unter Netware oder Linux auf einem separaten PC installiert werden.**
Bevor Sie DvSPAM in Ihrem Netzwerk installieren, legen Sie bitte fest wie sich der DvSPAM Service anmelden soll. Wählen Sie eine der folgenden Möglichkeiten:

1. Verwenden Sie den Administrator-Account für die Anmeldung des DvSPAM Service. Achten Sie auch hier auf die erforderlichen Rechte (s. 4.2).
2. Legen Sie manuell einen Account unter Windows für die Anmeldung des DvSPAM Service an und gewähren Sie diesem die erforderlichen Rechte (s. 4.2). Für eine David-Installation unter Netware oder Linux ist nur diese Variante möglich.

Vor Beginn der Installation von DvSPAM ist das Microsoft .NET Framework v2.0 zu installieren. Alternativ kann das Framework durch das Setup von Microsoft geholt und installiert werden.

Anschließend führen Sie das DvSPAM Setup aus und konfigurieren DvSPAM und den DvSPAM Service. Mit der Lizenzierung und dem Neustart des David Servicelayers wird die Installation abgeschlossen.

Beachten Sie, dass der Benutzer Account auch als David Benutzer eingerichtet sein muss.

4.2 Vorbereitung der Installation bei David unter Windows

Haben Sie im obigen Kapitel 4.1 die Variante 2 gewählt, führen Sie bitte die folgenden Schritte aus. Für die Variante 1 kontrollieren Sie bitte nur die Zugriffsrechte und die David Konfiguration.

Der DvSPAM Service benötigt zur Anmeldung im Netzwerk einen Account. Dieser **DvSPAM Service Account** muss das Recht „Vollzugriff“ auf die David Archive und das David\Code Verzeichnis erhalten, sowie Mitglied in der lokalen Gruppe der Administratoren sein.

Das Anlegen des **DvSPAM Service Accounts**, die Aufnahme des Accounts in die lokale Gruppe der Administratoren beziehungsweise die Gruppe der Domänen-Admins und die Vergabe der Rechte auf die David Archive nehmen Sie bitte wie folgt vor:

1. Legen sie einen Account für die Anmeldung des DvSPAM Service (**DvSPAM Service Account**) in der Windows-Domäne an. Verwenden Sie z.B. den Namen **DvSPAM**.

2. Nehmen sie den **DvSPAM Service Account** auf dem Server als Mitglied in die lokale Gruppe der Administratoren auf. Alternativ können Sie den **DvSPAM Service Account** in die Gruppe der Domänen-Administratoren aufnehmen.

3. Gewähren Sie dem **DvSPAM Service Account** das Recht „Vollzugriff“ auf alle David Archive und auf das Verzeichnis David\Code. Wenn Sie die erforderlichen Rechte manuell mit dem Kommando **CACLS** und der Option **/e** vergeben, bleiben alle bisher in den David Archiven gewährten Rechte erhalten. Gewähren Sie das Recht Vollzugriff für den **DvSPAM Service Account** gemäß dem folgenden Beispiel:

   cacls *Laufwerk*:**\david /t /e /g** *Domäne***dvspam:f**

   Die Beschreibung von **CACLS** finden Sie in der Windows-Hilfe.

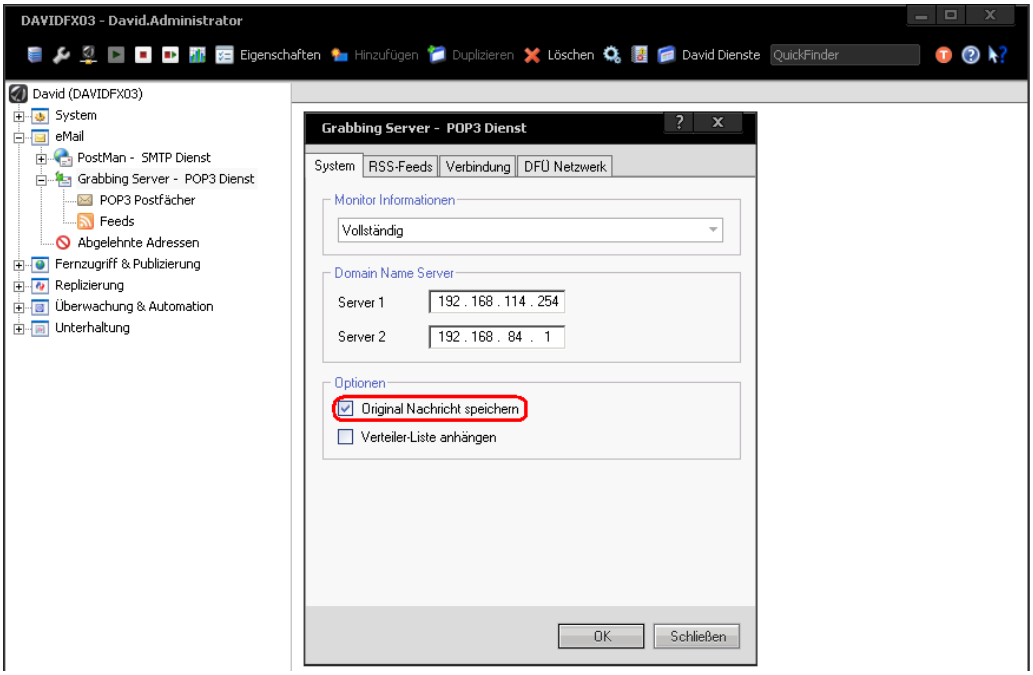
Wenn bei der David Installation für alle David Archive das Recht „Vollzugriff“ für die Gruppe der Administratoren gewährt wurde, können sie auf die explizite Vergabe von Rechten für den DvSPAM Service Account verzichten. Nehmen Sie in diesem Fall den DvSPAM Service Account auf dem David Server als Mitglied in die lokale Gruppe der Administratoren oder in die Gruppe der Domänen-Administratoren auf.

Konfiguration David:

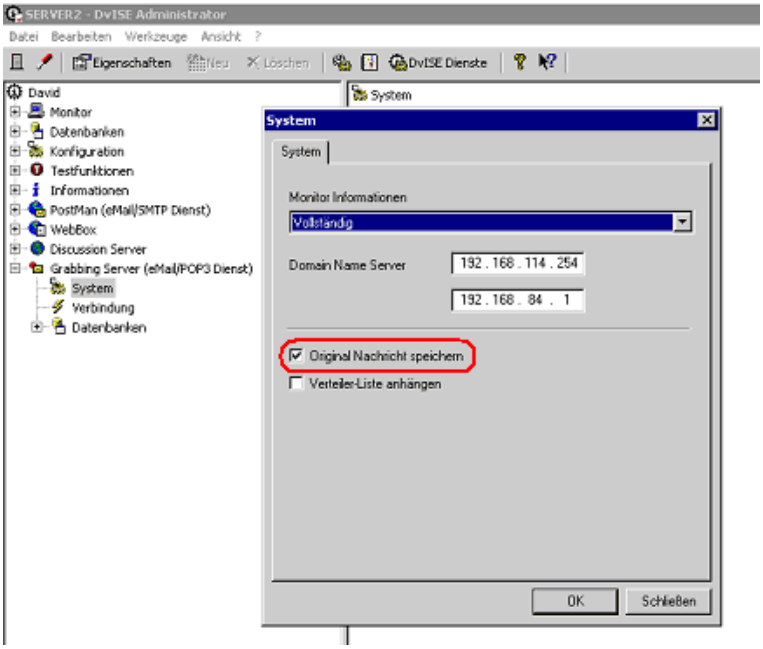
Aktivieren der Option „Original Nachricht speichern“

DvSPAM wertet, nach der Bewertung der White- und Blacklists, im NiXSpam Filter die komplette Nachricht aus. Hierzu ist es erforderlich, dass diese Nachricht im Original-Format vorliegt.

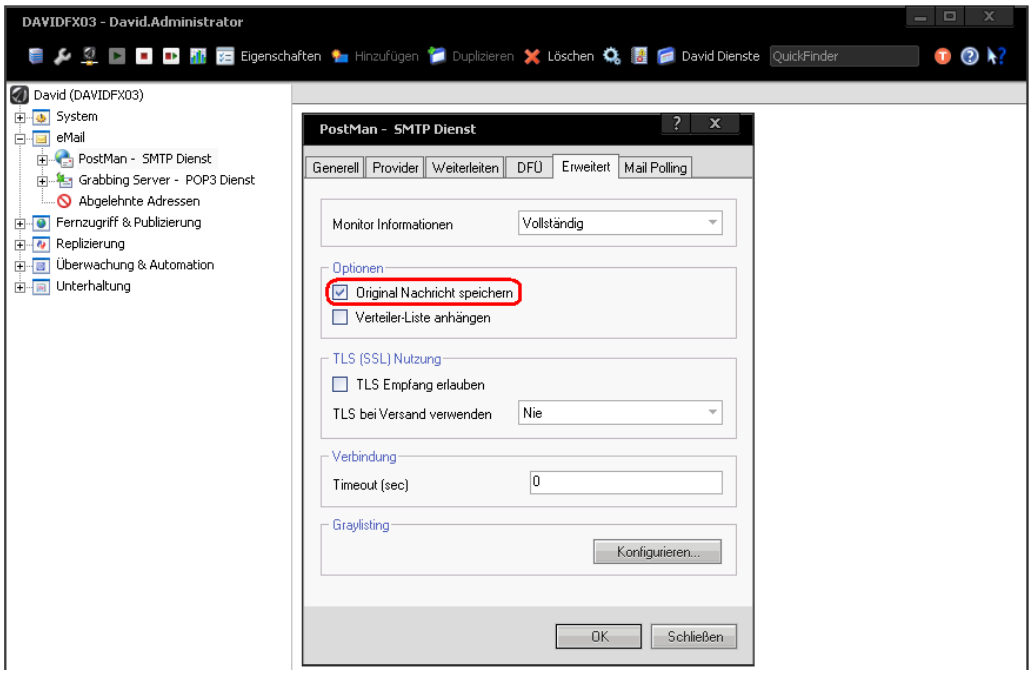
Dafür muss in dem für den Email-Empfang verantwortlichen David-Modul die Option **Original Nachricht speichern** aktiviert sein. Ruft David die Emails vom Provider per POP3 ab, konfigurieren Sie diese Option im **DvISE Grabbing Server**:



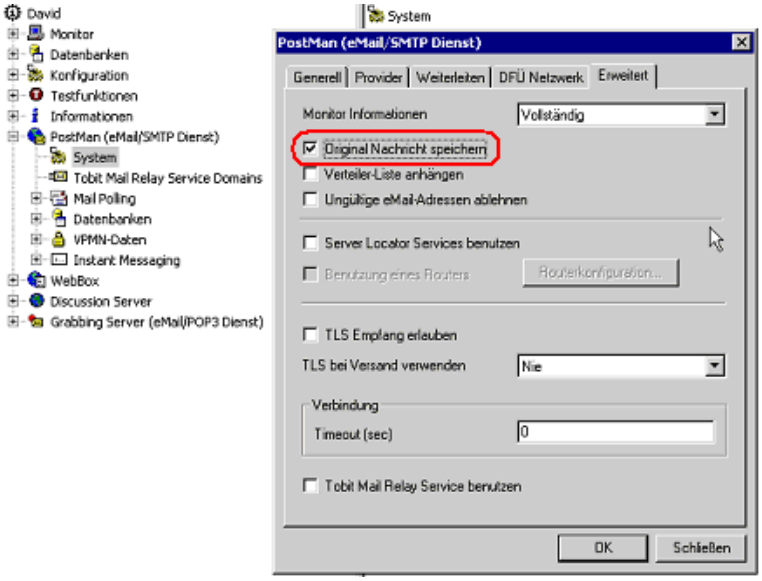
Oben die Konfiguration für David.fx12, unten für ältere Versionen:



Empfangen sie hingegen Ihre Nachrichten per SMTP, müssen Sie die genannte Option im **DvISE Postman** konfigurieren:



Oben die Konfiguration für David.fx12, unten für ältere Versionen:



4.3 Vorbereitung der Installation bei David unter Netware

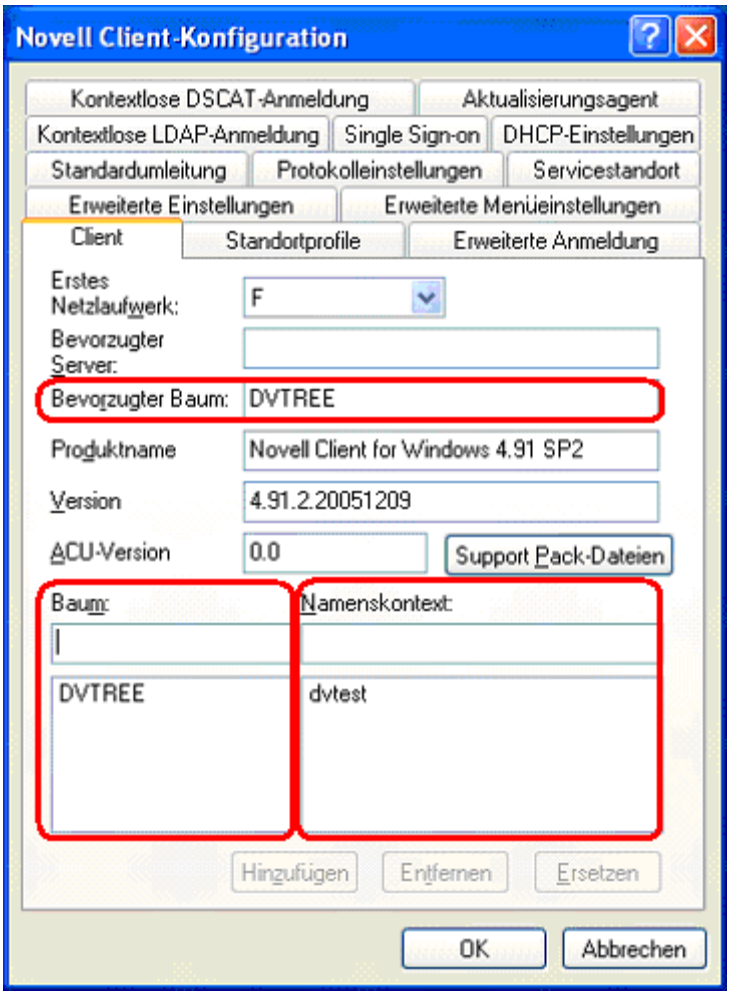
Für eine David Installation unter Netware sind die Varianten 1 und 2 möglich (s. 4.1). Wir empfehlen die Variante 1 nur zu verwenden, wenn es Probleme bei der Anmeldung mit der Variante 2 gibt.

Variante 1:
Der DvSPAM Service benötigt einen **DvSPAM Netware Account** zur Anmeldung im Netzwerk und einen **DvSPAM Service Account** zur lokalen Anmeldung auf der Windows Workstation. Beide Accounts können unterschiedliche Nutzernamen haben.
Führen Sie bitte die folgenden Schritte aus:

1. Legen Sie unter Netware einen Benutzer-Account (**DvSPAM Netware Account)** mit dem Namen „**dvspam**“ an, unter dem sich der **DvSPAM Service** unter Netware anmelden kann.
2. Gewähren Sie dem **DvSPAM Netware Account** die folgenden Rechte: **Read**, **Write**, **Modify, Create, File Scan** und **Erase** auf DAVID\ARCHIVE inklusive aller Unterverzeichnisse, auf DAVID\CODE und auf DAVID\APPS\FAXWARE\OUT\API. Alternativ können Sie auch einen vorhandenen Benutzer-Account verwenden, der die erforderlichen Rechte besitzt.
3. Legen Sie auf der für DvSPAM vorgesehenen Workstation einen Account für die Anmeldung des DvSPAM Service (**DvSPAM Service Account**) an. Nehmen Sie den **DvSPAM Service Account** auf dieser Workstation in die lokale Gruppe der Administratoren auf. Alternativ kann wie bei der Installation unter Windows auch der Administrator Account verwendet werden.
4. Der DvSPAM Service muss sich am Netware Server anmelden. Diese Anmeldung erfolgt mit einem Kommandozeilenlogin, welches extra zu installieren ist. Sie finden das Setup im Unterverzeichnis install im DvSPAM Programmverzeichnis (HBWlogin103.exe). Installieren Sie es bitte und kopieren Sie danach den Inhalt des Verzeichnisses HBware/HBWlogin in das DvSPAM Programmverzeichnis. Zur weiteren Konfiguration von HBWlogin verwenden Sie bitte die dort mitgelieferte Dokumentation.
   Der DvSPAM Service überprüft die Verfügbarkeit der Datei hbwlogin.exe im Programmverzeichnis und verwendet dann die alternative Anmeldung an den Netware Server.
5. Nach dem Starten des DvSPAM Service kontrollieren Sie bitte den Monitor bzw. die Logdatei. Unmittelbar nach dem Starten überprüft der Service die notwendigen Schreib- und Leserechte und schreibt bei Problemen entsprechende Logeinträge.

Variante 2:
Der DvSPAM Service benötigt einen **DvSPAM Netware Account** zur Anmeldung im Netzwerk und einen **DvSPAM Service Account** zur lokalen Anmeldung auf der Windows Workstation. Beide Accounts müssen den gleichen Nutzernamen und das gleiche Passwort haben.
Führen Sie bitte die folgenden Schritte aus:

1. Legen Sie unter Netware einen Benutzer-Account (**DvSPAM Netware Account)** mit dem Namen „**dvspam**“ an, unter dem sich der **DvSPAM Service** unter Netware anmelden kann. Das hier verwendete Kennwort muss mit dem später unter Windows verwendeten (Punkt 4) identisch sein.
2. Gewähren Sie dem **DvSPAM Netware Account** die folgenden Rechte: **Read**, **Write**, **Modify, Create, File Scan** und **Erase** auf DAVID\ARCHIVE inklusive aller Unterverzeichnisse, auf DAVID\CODE und auf DAVID\APPS\FAXWARE\OUT\API.
3. Für eine korrekte Anmeldung des DvSPAM-Service unter Netware ist eine Konfiguration der Client - Eigenschaften des Novell Netware-Clients erforderlich. Geben sie in der Novell Client Konfiguration auf der Registerkarte „Client“ den „Preferred Tree“ sowie „Tree“ und „Name context“ wie in der Abbildung ersichtlich an:



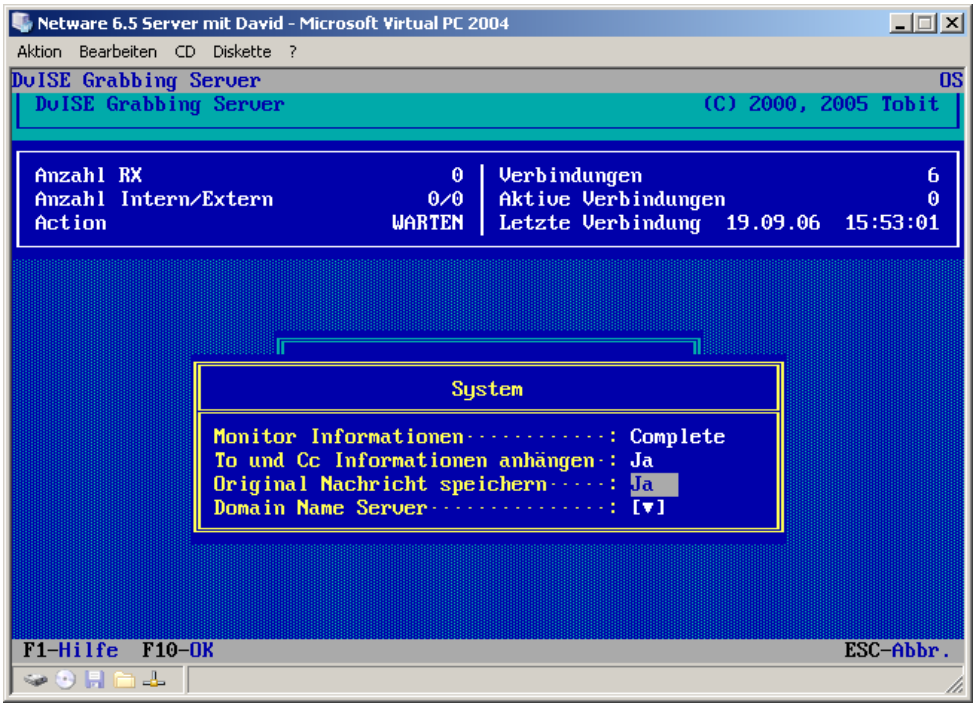
4. Legen Sie auf der für DvSPAM vorgesehenen Workstation einen Account für die Anmeldung des DvSPAM Service (**DvSPAM Service Account**) an. Verwenden Sie den gleichen Benutzernamen und das gleiche Kennwort wie für den **DvSPAM Netware Account**. Nehmen Sie den **DvSPAM Service Account** auf dieser Workstation in die lokale Gruppe der Administratoren auf.

Konfiguration David:

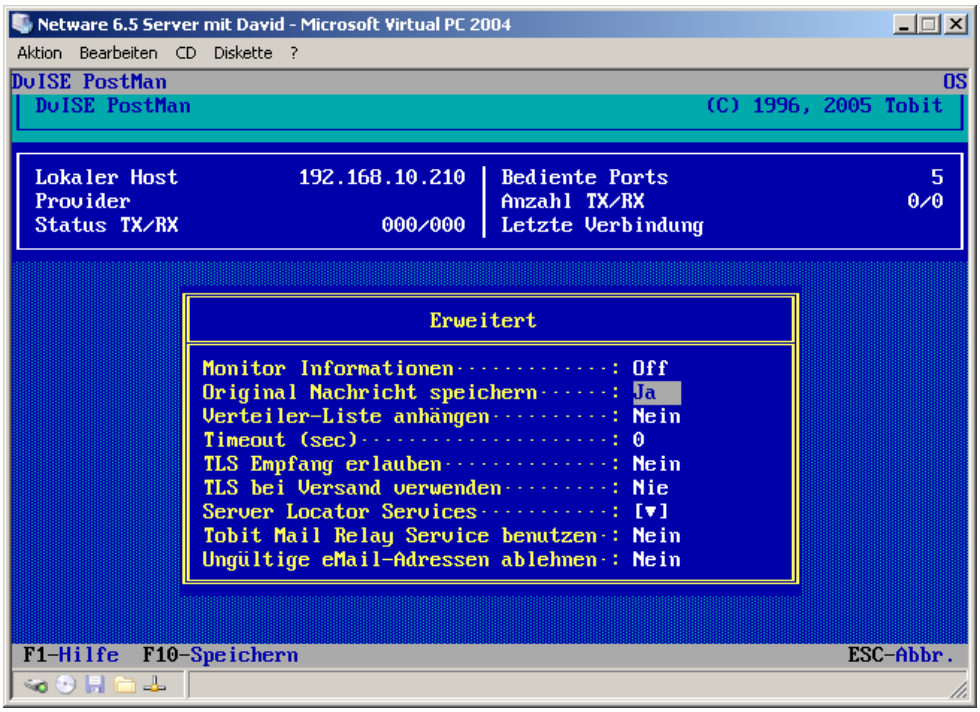
Aktivieren der Option „Original Nachricht speichern“

DvSPAM wertet, nach der Bewertung der White- und Blacklists, im NiXSpam Filter die komplette Nachricht aus. Hierzu ist es erforderlich, dass diese Nachricht im Original-Format vorliegt.

Dafür muss in dem für den Email-Empfang verantwortlichen David-Modul die Option **Original Nachricht speichern** aktiviert sein. Ruft David die Emails vom Provider per POP3 ab, konfigurieren Sie diese Option im **DvISE Grabbing Server**:



Empfangen sie hingegen Ihre Nachrichten per SMTP, müssen Sie die genannte Option im **DvISE Postman** konfigurieren:



4.4 Vorbereitung der Installation bei David unter Linux

Für eine David Installation unter Linux ist nur die Variante 2 möglich (s. 4.1).

Der DvSPAM Service benötigt zur Anmeldung unter Linux zwei **DvSPAM Linux** und **SAMBA Accounts** und einen gleichnamigen lokalen **DvSPAM Service Account** auf der Windows Workstation.

Das Anlegen und die Konfiguration der **DvSPAM Service, Linux** und **SAMBA Accounts** nehmen Sie bitte wie folgt vor:

1. Legen Sie unter Linux und unter SAMBA Benutzer-Accounts (**DvSPAM Linux Account** und **DvSPAM SAMBA Account**) mit dem Namen „**dvspam**“ an. Das hier verwendete Kennwort muss mit dem später unter Windows verwendeten (Punkt 3) identisch sein. Der Benutzer „**dvspam**“ ist Mitglied der Gruppe **root** und der zugriffsberechtigten SAMBA-Gruppe der Tobit David Share.
2. In der david.ini den Eintrag ´AutoValidation = FALSE´ setzten und den Servicelayer neu starten ´DvISEctl restart sl´
3. Gewähren Sie den **DvSPAM Linux** und **SAMBA Accounts** volle Schreib- und Leserechte auf DAVID\ARCHIVE inklusive aller Unterverzeichnisse, auf DAVID\CODE und auf DAVID\APPS\FAXWARE\OUT\API.
4. Legen Sie auf der für DvSPAM vorgesehenen Workstation einen Account für die Anmeldung des DvSPAM Service (**DvSPAM Service Account**) an. Verwenden Sie den gleichen Benutzernamen und das gleiche Kennwort wie für die **DvSPAM Linux** und **SAMBA Accounts**. Nehmen Sie den **DvSPAM Service Account** auf dieser Workstation in die lokale Gruppe der Administratoren auf.

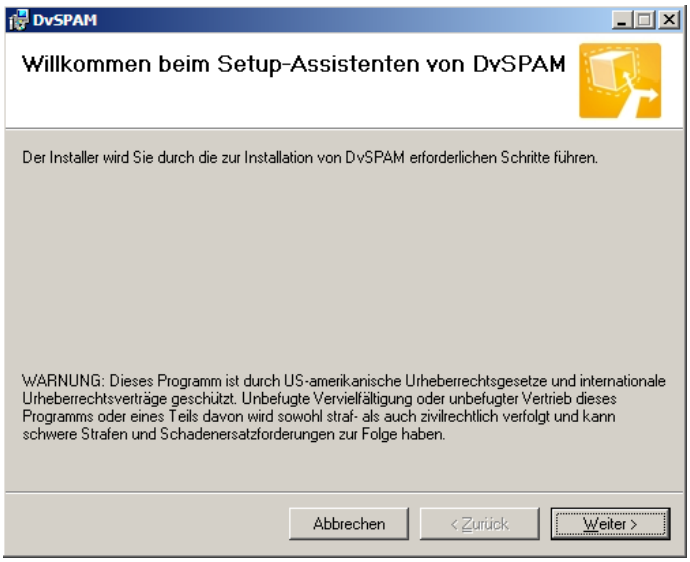
Nach der Installation von DvSPAM sind weitere Linux-spezifische Einstellungen notwendig (s. 5.12).

4.5 Installation

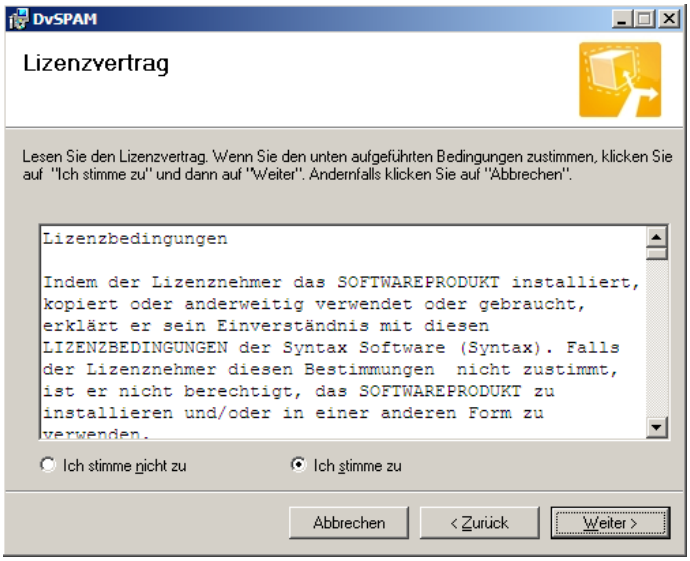
Nach der Installation von .NET Framework können Sie nun DvSPAM installieren. Das DvSPAM Setup entnimmt der Konfiguration des David Clients einige notwendige Informationen.

Vor der Ausführung des Setups müssen unbedingt die Schritte zur Vorbereitung gemäß Kapitel 4.2-4.4 durchgeführt werden!

Zur Installation von DvSPAM führen Sie bitte die Datei **Setup.exe** aus:

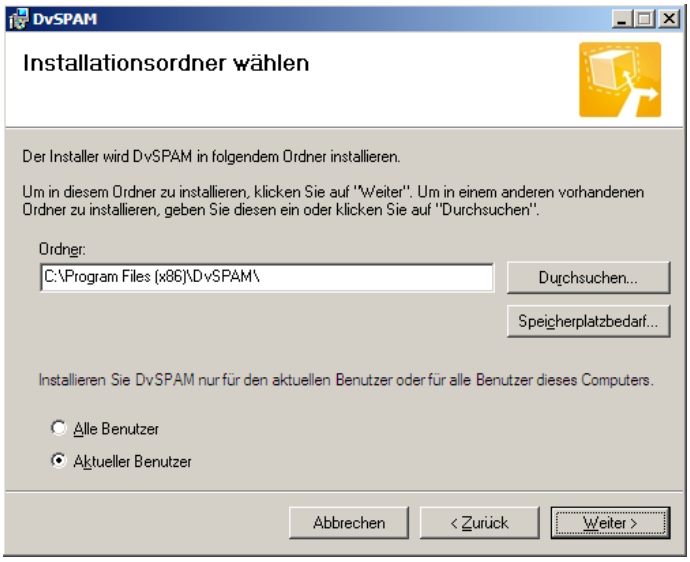

DvSPAM
Willkommen beim Setup-Assistenten von DvSPAM
Der Installer wird Sie durch die zur Installation von DvSPAM erforderlichen Schritte führen.
WARNUNG: Dieses Programm ist durch US-amerikanische Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt. Unbefugte Vervielfältigung oder unbefugter Vertrieb dieses Programms oder eines Teils davon wird sowohl straf- als auch zivilrechtlich verfolgt und kann schwere Strafen und Schadenersatzforderungen zur Folge haben.
Abbrechen
< Zurück
Weiter >

Klicken Sie auf **weiter**, um mit der Installation zu beginnen. Lesen Sie bitte sorgfältig die Lizenzvereinbarung für DvSPAM:


DvSPAM
Lizenzvertrag
Lesen Sie den Lizenzvertrag. Wenn Sie den unten aufgeführten Bedingungen zustimmen, klicken Sie auf "Ich stimme zu" und dann auf "Weiter". Andernfalls klicken Sie auf "Abbrechen".
Lizenzbedingungen
Indem der Lizenznehmer das SOFTWAREPRODUKT installiert, kopiert oder anderweitig verwendet oder gebraucht, erklärt er sein Einverständnis mit diesen LIZENZBEDINGUNGEN der Syntax Software (Syntax). Falls der Lizenznehmer diesen Bestimmungen nicht zustimmt, ist er nicht berechtigt, das SOFTWAREPRODUKT zu installieren und/oder in einer anderen Form zu verwenden.
Ich stimme nicht zu
Ich stimme zu
Abbrechen
< Zurück
Weiter >

Sie sind berechtigt, DvSPAM als SPAM Filter für einen David-Server zu installieren. Dazu müssen Sie für DvSPAM mindestens so viele Benutzerlizenzen erworben haben, wie für diesen David Server David Benutzerlizenzen installiert sind. Wenn Sie mit den Lizenzbedingungen einverstanden sind, wählen Sie **Ich stimme zu**. Wählen sie **Ich stimme nicht zu** um die Installation zu beenden.

Wählen Sie nun das Installationsverzeichnis:


DvSPAM
Installationsordner wählen
Der Installer wird DvSPAM in folgendem Ordner installieren.
Um in diesem Ordner zu installieren, klicken Sie auf "Weiter". Um in einem anderen vorhandenen Ordner zu installieren, geben Sie diesen ein oder klicken Sie auf "Durchsuchen".
Ordner:
C:\Program Files (x86)\DvSPAM\
Durchsuchen...
Speicherplatzbedarf...
Installieren Sie DvSPAM nur für den aktuellen Benutzer oder für alle Benutzer dieses Computers.
Alle Benutzer
Aktueller Benutzer
Abbrechen
< Zurück
Weiter >

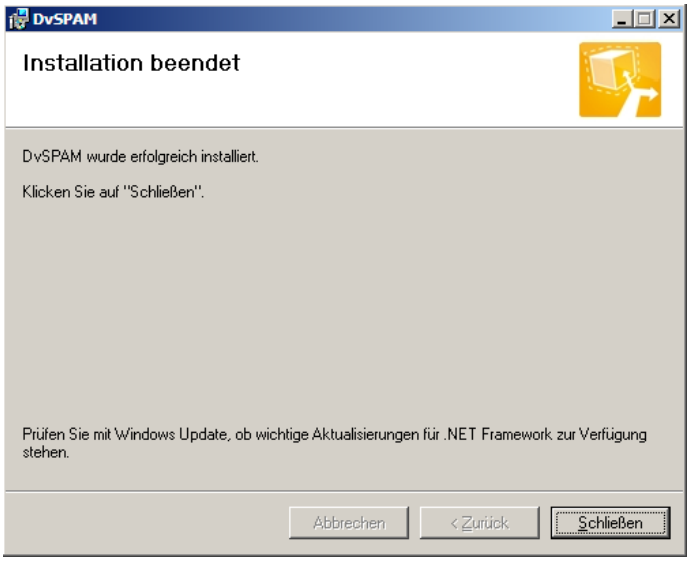
und klicken Sie auf **weiter**.

Folgen sie den folgenden Dialogen. Änderungen an den vorgeschlagenen Optionen sind nicht notwendig.

Bitte kontrollieren Sie, ob die Optionen Original Nachricht speichern im Postman und/oder Grabbing Server aktiviert sind und bestätigen Sie die folgende Dialogbox:

DvSpam Install
Bitte kontrollieren Sie die Installation bzw. Konfiguration der folgenden Punkte entsprechend dem Handbuch:
Bitte aktivieren Sie die Option 'Original-Nachricht speichern' im DvISE Administrator (Postman bzw. Grabbingserver).
Bitte starten Sie jetzt oder zu einem spätern Zeitpunkt den David-Servicelayer neu damit die Konfigurationsänderungen von David übernommen werden.
Hinweis: Die automatische Whitelist arbeitet erst nach diesem Neustart.
OK

Hiermit ist die Installation von DvSPAM beendet. Starten Sie den ServiceLayer einmal neu.



Sie haben nun DvSPAM als unlizenzierte Demo-Version installiert. Der DvSPAM Service lässt sich in diesem Modus nicht starten. Es besteht aber die Möglichkeit, die Oberfläche kennen zu lernen und manuell (per Kontextmenü im David Client) eine Nachricht zu prüfen. Wollen Sie DvSPAM als Vollversion oder als 30Tage-Demo-Version betreiben, führen Sie bitte eine Lizenzierung durch.

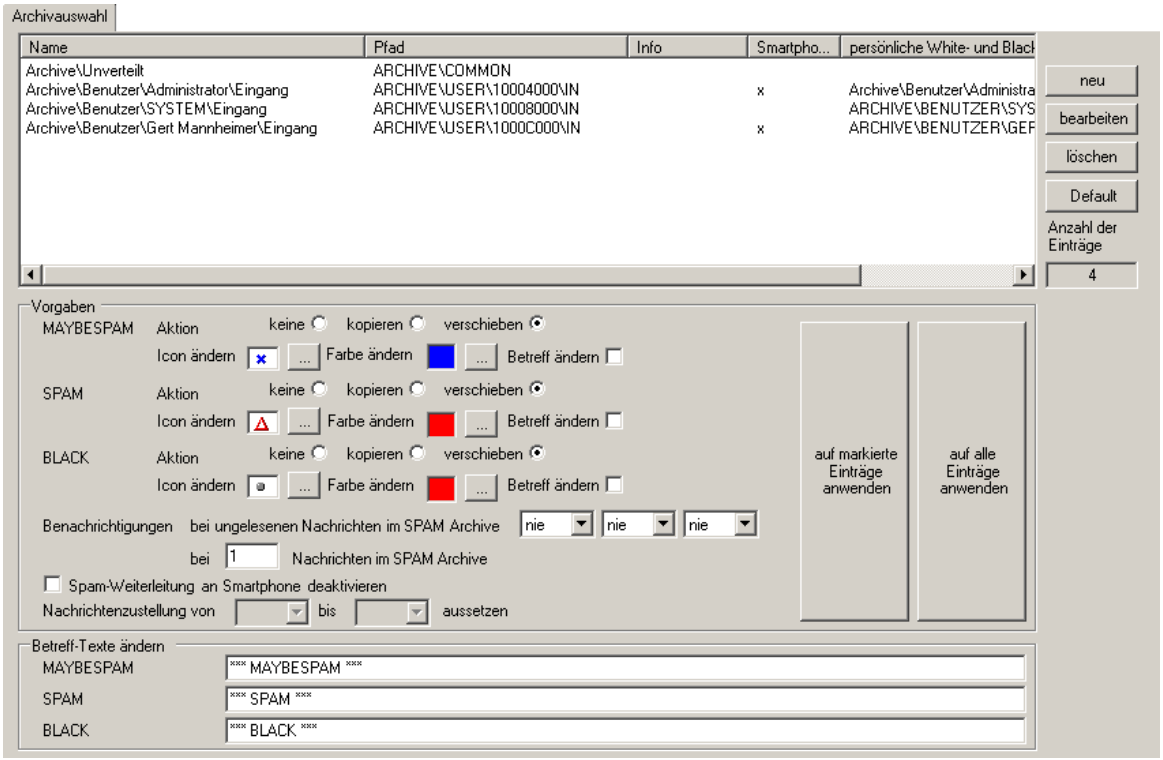
5 Konfiguration

5.1 Registerkarte Archivauswahl

DvSPAM untersucht alle Nachrichten, die von David in einem der konfigurierten Eingangsarchive abgelegt werden. Nach der Klassifizierung als HAM, MAYBESPAM, SPAM, WHITE und BLACK werden eine oder mehrere der konfigurierten Aktionen durchgeführt:

- **HAM, WHITE: Die erwünschten Nachrichten bleiben unverändert im Eingangsarchiv liegen.**
- **MAYBESPAM, SPAM, BLACK**: Für alle drei Klassifizierungen können gleiche Aktionen konfiguriert werden. Folgende Aktionen sind konfigurierbar:
  - Die Nachricht kann in ein zu konfigurierendes Archiv kopiert oder verschoben werden. Default-Wert sind bei den Benutzer-Archiven und im Archiv **Unverteilt** jeweils das David-SPAM-Archiv, welches ab David XL von David angelegt wird.
  - Das Flag der Nachricht kann gesetzt werden.
  - Die Farbe des Eintrags der Nachricht kann geändert werden.
  - Am Anfang des Betreffs kann ein Text eingefügt werden. Dieser wird global auf der Registerkarte **Konfiguration** vorgegeben.

Auf der Registerkarte **Archivauswahl** werden die Eingangsarchive und die nach der Klassifizierung der Emails durch DvSPAM durchzuführenden Aktionen konfiguriert. Es ist jeweils möglich, einen Eintrag über das Kontextmenü oder über die Buttons am rechten Fensterrand zu bearbeiten:



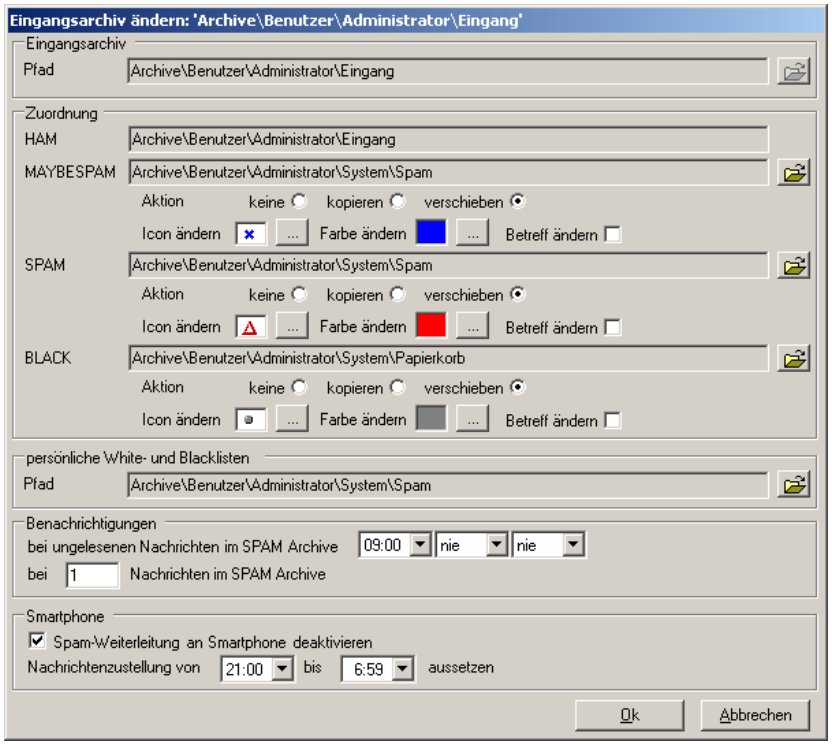
- **Neu**: Es wird ein neues Eingangsarchiv mit den dazugehörigen Aktionen angelegt. Dabei werden die unter **Vorgaben** konfigurierten Einstellungen verwendet.

- **Löschen**: Der ausgewählte Eintrag wird gelöscht.

- **Default**: Durch diesen Menüpunkt wird entweder die aktuelle Archivauswahl gelöscht und mit einer Default- Konfiguration neu angelegt oder die aktuelle Archivauswahl um diese Default-Konfiguration ergänzt. Die Default-Konfiguration enthält das Zentraleingangs- bzw. Unverteilt-Archiv und die Eingangsarchive aller David-Benutzer. Dabei werden die unter **Vorgaben** konfigurierten Einstellungen verwendet.

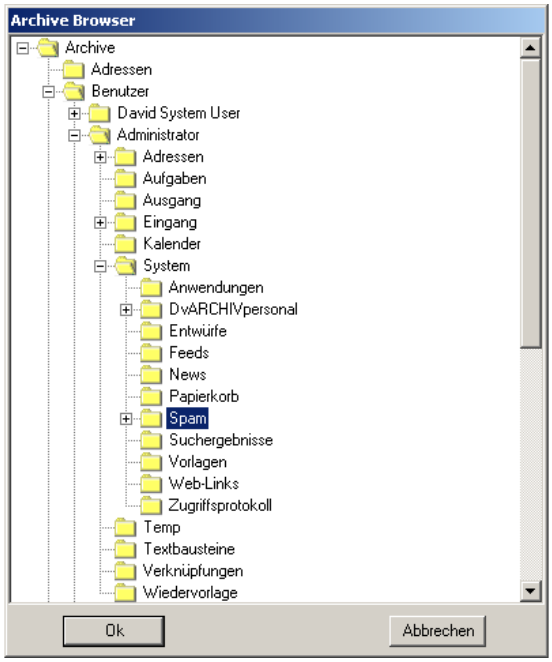
- Ein **Doppelklick** öffnet die Archive zur Konfiguration:

- **Betreff Texte:** Diese Ergänzungen des Betreff-Textes werden für die entsprechende Aktion nach einer Mailklassifizierung verwendet.



Die Eingangs- und die Ablagearchive sind konfigurierbar. Sind die Ablagearchive (z.B. die SPAM-Archive in David 6.6 bzw. bei David unter Netware und Linux) noch nicht vorhanden, werden diese durch den DvSPAMadministrator in den Nutzerarchiven unter System bzw. direkt unter Unverteilt angelegt. Die persönlichen White- und Blacklisten werden beim Speichern der Konfiguration ebenfalls unterhalb des ausgewählten Pfades angelegt.

Die Auswahl erfolgt jeweils über den Browse-Button.



Das SPAM Archive sollte regelmäßig auf falsch erkannte Nachrichten überprüft werden. Zur Erinnerung kann eine Nachricht im Nutzereingang abgelegt werden. Dies ist zu einer bestimmten Uhrzeit möglich. Die Nachricht enthält dabei Informationen über die nicht gelesenen SPAM Nachrichten. Alternativ kann auch eine Erinnerung ab einer bestimmten Gesamtanzahl von Nachrichten im SPAM Archiv erzeugt werden.

Vorgaben:

- **MAYBESPAM**: Legen Sie hier die MAYBESPAM-Vorgaben für neue Einträge fest. Die Vorgabe gilt für alle neuen Einträge, egal ob sie mit dem Button **neu** oder **Default** angelegt werden.

- **SPAM**: Legen Sie hier die SPAM-Vorgaben für neue Einträge fest. Die Vorgabe gilt für alle neuen Einträge, egal ob sie mit dem Button **neu** oder **Default** angelegt werden.

- **BLACK**: Legen Sie hier die BLACK-Vorgaben für neue Einträge fest. Die Vorgabe gilt für alle neuen Einträge, egal ob sie mit dem Button **neu** oder **Default** angelegt werden.

- **Benachrichtigungen:** Hier können Sie bis zu drei verschiedene Zeitpunktpunkte konfigurieren, zu denen Sie bei einer bestimmten Anzahl an Nachrichten im SPAM-Verzeichnis informiert werden wollen. Diese Benachrichtigung erfolgt im entsprechenden Benutzer-Eingang.

- **Smartphone:** Hier können Sie einstellen, dass eingehende Nachrichten per Regel direkt in einen separaten Transfer-Ordner verschoben werden. In diesem „In Spamprüfung“ Ordner, der automatisch unterhalb des Eingangsarchives angelegt wird, erfolgt anschließend die Klassifizierung und Verteilung durch DvSPAM. Diese Funktion unterbindet die Smartphone Push Notifizierung für unerwünschte Nachrichten. Außerdem haben Sie zusätzlich die Möglichkeit, die SPAM-Prüfung bzw. Weiterleitung von Nachrichten in einem bestimmten Zeitraum generell pausieren zu lassen.

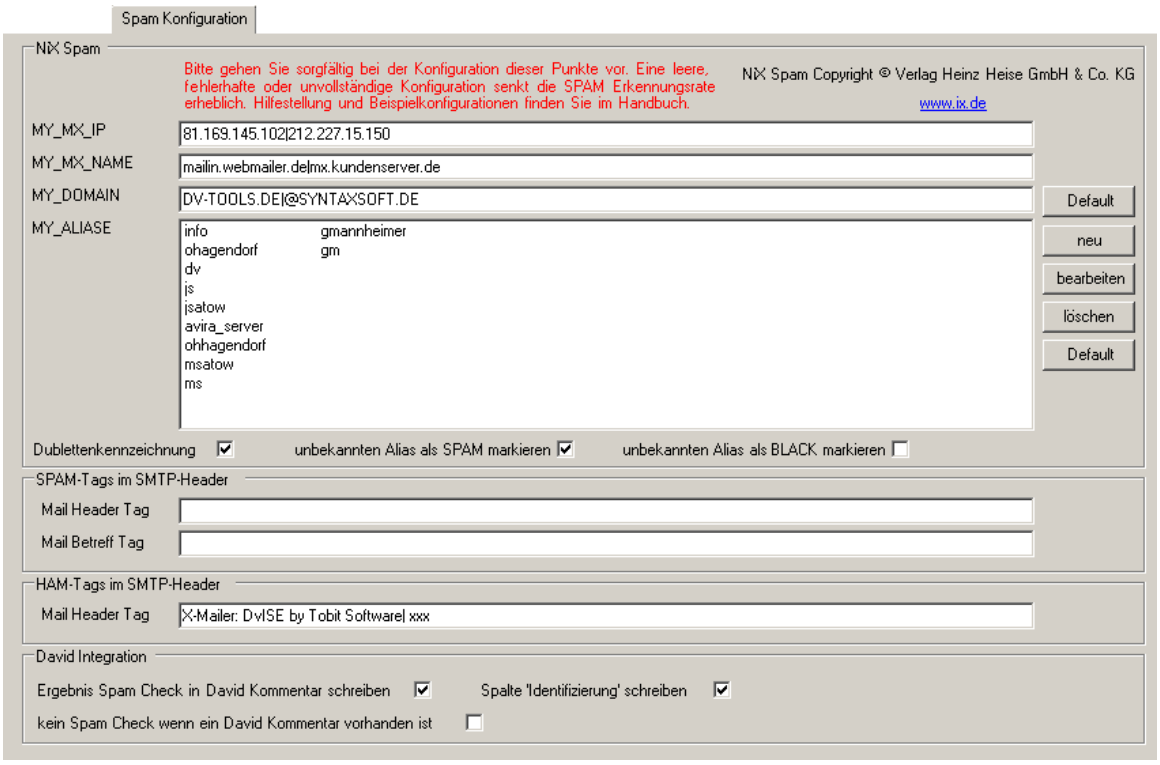
- Button **Auf markierte Einträge anwenden**: Über diese Schaltfläche können Sie die oben beschriebenen Einstellungen nachträglich für alle in der Archivauswahl markierten Einträge ändern.

- Button **Auf alle Einträge anwenden**: Über diese Schaltfläche können Sie die oben beschriebenen Einstellungen nachträglich für alle Einträge ändern.

Es ist nicht möglich, aufgrund eines durch den Spam Filter geänderten Betrefftextes oder einer verschobenen Nachricht regelbasiert Aktionen durch David selbst durchzuführen. Alle konfigurierten Regeln wurden bereits vor der Spam Prüfung abgearbeitet.
Beim Deaktivieren der Spam-Weiterleitung ans Smartphone werden existierende Regeln in den Ordner 'In Spamprüfung' Ordner verschoben. Nach erneuter Aktivierung werden diese Regeln nicht automatisch zurück kopiert; dies muss manuell durchgeführt werden.
Ist die Spam-Weiterleitung deaktiviert, achten Sie bitte darauf, dass neue Regeln ausschließlich im 'In Spamprüfung'-Archive angelegt werden sollten.

5.2 Registerkarte Spam Konfiguration

Auf der Registerkarte **Spam Konfiguration** werden alle für die Klassifizierung notwendigen Angaben konfiguriert:



NiX Spam:

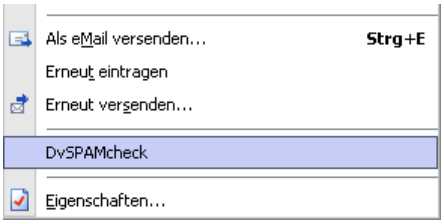
- **MY_MX_IP, MY_MX_NAME:** Beide Angaben finden Sie, indem Sie auf der Maschine, auf der DvSPAM installiert ist, **DvSPAMcheck** aufrufen. Alternativ können Sie im David Client den Dialog ***Erweiterte Information*** (Kontext-Menü einer Mail) /*Eigenschaften*/Button *Erweitert…*/Anzeige *SMTP Header*) verwenden.

  Verwendung von Wildcards in MY_MX_NAME

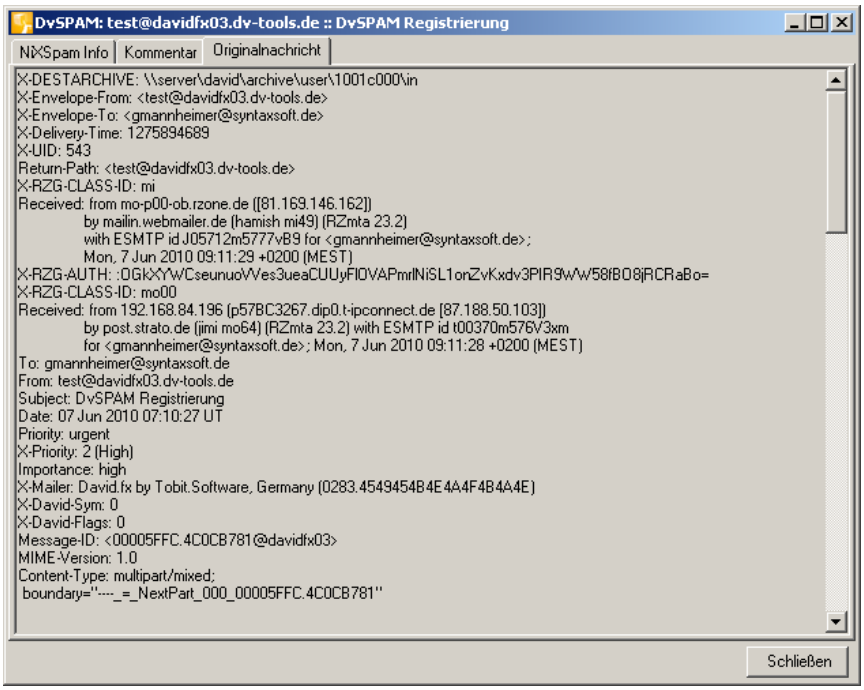
  Einige Provider verwenden mehrere Mailserver, die sich nur durch eine Nummer im Namen unterscheiden. In diesem Fall können Sie einen regulären Ausdruck für die Nummern verwenden, z.B. *mailserver[0-9][0-9].domain.de* für alle Mailserver von mailserver00.domain.de – mailserver99.domain.de Unterscheiden sich die Mailservernamen nur durch wenige Buchstaben kann Sie *[a-z]* für einen Buchstaben oder *[a-z]+* für einen oder mehrere Buchstaben angeben.

  Werden diese beiden Punkte nicht korrekt konfiguriert, werden alle Mails mit Ausnahme der Blacklist, Betreff und Header Tag Erkennung als interne Nachrichten und damit als HAM klassifiziert.

DvSPAMcheck rufen Sie wie folgt auf: Klicken Sie im David Client auf dem David-Server mit der rechten Maustaste auf eine empfangene externe Nachricht und wählen sie im Kontextmenü den Eintrag **DvSPAMcheck**.



DvSPAMcheck dient allgemein der Diagnose der Funktionen von DvSPAM.



Auf der Registerkarte **Originalnachricht** von DvSPAMcheck suchen Sie in den Received-Abschnitten den 1. Block, der mit (**E**)**SMTP** empfangen wurde. Aus diesem Block übertragen Sie den Namen des Mail-Servers und dessen IP-Adresse in die dazugehörigen Felder im DvSPAMadministrator. Hierzu finden Sie unten drei Beispiele.

Werden die Mails per POP von einem Provider abgeholt ist i.d.R. dieselbe IP Adresse wie in der POP Konten Definition zu verwenden.
Werden die Mails per SMTP empfangen ist i.d.R. die öffentliche IP Adresse des SMTP Servers zu verwenden.

Beispiel 1:
Im 1. Beispiel holt der David-Server die Nachrichten von dem POP3 Server des Providers. Der 1. Block zeigt den Empfang der Nachricht per (**E**)**SMTP** durch den Mailserver ***mailin.webmailer.de***. Dieser Name muss im DvSPAMadministrator unter **MY_MX_NAME** eingetragen werden.

```
X-DESTARCHIVE: \\vpc1\david\archive\user\10008000\in
X-Envelope-From: <olaf.hagendorf@lycos.de>
X-Envelope-To: <ohagendorf@syntaxsoft.de>
X-Delivery-Time: 1164622679
Received: from lmfilto01.st1.spray.net (lmfilto01.st1.spray.net
    [212.78.202.65])
    by mailin.webmailer.de (8.13.7/8.13.7) with ESMTP id kARAHw2U027606
    for <ohagendorf@syntaxsoft.de>; Mon, 27 Nov 2006 11:17:58 +0100 (MET)
Received: from lmfilto01.st1.spray.net (localhost [127.0.0.1])
    by lmfilto01-10027.st1.spray.net (Postfix) with ESMTP id E55BBB9C18E
    for <ohagendorf@syntaxsoft.de>; Mon, 27 Nov 2006 10:17:57 +0000 (GMT)
Received: from localhost (localhost [127.0.0.1])
    by lmfilto01-10025.st1.spray.net (Postfix) with ESMTP id BD13DB9BDFD
    for <ohagendorf@syntaxsoft.de>; Mon, 27 Nov 2006 10:17:57 +0000 (GMT)
Received: from cmcodec06.st1.spray.net (localhost [127.0.0.1])
    by cmcodec06.st1.spray.net (Postfix) with SMTP id 67C2010D68C
    for <ohagendorf@syntaxsoft.de>; Mon, 27 Nov 2006 10:17:57 +0000 (GMT)
Comment: DomainKeys? See http://antispam.yahoo.com/domainkeys
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=beta; d=lycos.de;
```

Beispiel 2:
Im 2. Beispiel holt der David-Server die Nachrichten von einem internen POP3 Server. Diese Kommunikation zeigt der 1. Received-Block. Der 2. Block zeigt den Empfang der Nachricht per (**E**)**SMTP** durch den Mailserver ***mailin.webmailer.de***. Dieser Name muss im DvSPAMadministrator unter **MY_MX_NAME** eingetragen werden.

```
X-DESTARCHIVE: david\archive\user\10018010\in
X-KENId: 00007137KEN12E4642D
Received: from 192.67.198.62:110
    by KEN! (192.168.114.254:2538) with POP3
    ; Tue, 1 Nov 2005 10:30:06 +0100
Received: from kundenserver.de (sos-softwareshop.de [212.227.83.147])
    by mailin.webmailer.de (8.13.1/8.13.1) with ESMTP id jA19PsEh007843
    for <OHagendorf@Syntaxsoft.de>; Tue, 1 Nov 2005 10:25:55 +0100 (MET)
Received: from 192.168.10.10 by systeam-net.de
    (MDaemon.PRO.v7.2.0.R)
    with ESMTP id md50001113723.msg
    for <OHagendorf@Syntaxsoft.de>; Tue, 01 Nov 2005 10:23:44 +0100
Date: Tue, 1 Nov 2005 09:25:48 +0000
From: "Jobst-Peter Fischer" jpfischer@systeam.cc
```

Beispiel 3:
Im 3. Beispiel empfängt der David-Server die Nachrichten vom POP3 Server des Providers, der diese direkt per SMTP empfangen hat.

```
X-SMTPTOFIELD: X-MDRcpt-To
Return-path: <OHagendorf@Syntaxsoft.de>
Received: from natsmtp00.rzone.de (natsmtp00.rzone.de [81.169.145.165])
   by systeam-net.de (systeam-net.de [213.217.73.133])
   (MDaemon.PRO.v7.2.0.R) with ESMTP id md50001245607.msg
   for <david@systeam-hl.de>; Wed, 07 Dec 2005 18:55:59 +0100
Received: from 192.168.84.2 (p548C75CF.dip.t-dialin.net [84.140.117.207])
   by post.webmailer.de (8.13.1/8.13.1) with ESMTP id jB7Hv8TA021219
   for <jpfischer@systeam.cc>; Wed, 7 Dec 2005 18:57:10 +0100 (MET)
From: "OlafHagendorf"<OHagendorf@Syntaxsoft.de>
Subject: DvSPAM 1.0.13
To: jpfischer@systeam.cc
Date: Wed, 7 Dec 2005 17:57:09 +0000
Priority: normal
X-Priority: 3 (Normal)
Importance: normal
X-Mailer: DvISE by Tobit Software, Germany (0228.434B4A4D4A47474F4D4B), Mime
Converter 101.20
```

Die IP-Adresse lässt sich durch ein **ping** auf diesen Server ermitteln. Die so gewonnene IP-Adresse tragen Sie in das Feld **MY_MX_IP** ein. Sollten mehrere Namen und/oder Adressen verwendet werden, sind diese durch Semikolon oder einen senkrechten Strich (Pipe Symbol) getrennt hintereinander einzutragen.
Beispiel: *192.67.198.48*; *192.67.198.37*; *192.67.198.23* bzw. mailin.webmailer.de;mx.kundenserver.de

- **MY_DOMAIN:** Tragen Sie hier alle von Ihnen verwendeten Mail Domänen jeweils mit einem voran gestellten @ und durch ein Semikolon oder einen senkrechten Strich (Pipe Symbol) getrennt ein. Beispiel: *@dvspam.de*;*@dv-tools.de*. Mit dem Default Button versucht der DvSPAMadministrator alle verwendeten Domains aus der David Konfiguration auszulesen. Bitte kontrollieren Sie die ermittelten Domains und korrigieren diese gegebenenfalls.

- **MY_ALIASE:** Diese Liste enthält alle von Ihnen verwendeten Aliase, also alle in den Email-Adressen links vom @ verwendeten Namen. Verwendet beispielsweise ein Nutzer die beiden Mailadressen *fschulze@dv-tools.de* und *fs@dv-tools.de*, müssen die Aliase *fschulze* und *fs* eingetragen werden. Mit dem Default Button versucht der DvSPAMadministrator alle verwendeten Aliase aus der David Konfiguration auszulesen. Bitte kontrollieren Sie die ermittelten Aliase und korrigieren diese gegebenenfalls.

Für die **MY_MX_IP**, **MY_MX_NAME**, **MY_DOMAIN** und **MY_ALIAS** sind nur bestimmte Zeichen erlaubt:

- MX_IP: Ziffer, Punkt, Semikolon, Pipe
- MX_NAME: Ziffer, Buchstabe, Bindestrich, Punkt, Semikolon, Pipe, eckige Klammern
- DOMAIN: Ziffer, Buchstabe, Bindestrich, Punkt, Semikolon, Pipe
- ALIAS: Ziffer, Buchstabe, Bindestrich, Unterstrich, Punkt, Semikolon, Pipe

- **Dublettenkennzeichnung:** Wenn diese Option aktiviert ist, merkt sich DvSPAM zu empfangenen Emails bestimmte, eindeutige Eigenschaften. Wird eine zweite, identische Email empfangen, erhält sie eine negativere Bewertung. Diese Bewertung alleine ist noch nicht ausreichend, die Nachricht als SPAM zu kennzeichnen, erhöht aber die Wahrscheinlichkeit dafür deutlich. Verwenden Sie in Ihrem David Server Verteilregeln, die eine Mail an mehrere Nutzer verteilt, sollten Sie diese Option nicht aktivieren, da dadurch die Fehlerkennungsrate steigen kann.

- **unbekannten Alias als SPAM markieren:** Wird eine Email mit einem nicht konfigurierten Alias empfangen und diese Option ist aktiviert, wird diese Nachricht als SPAM markiert.

- **unbekannten Alias als BLACK markieren:** Wird eine Email mit einem nicht konfigurierten Alias empfangen und diese Option ist aktiviert, wird diese Nachricht als BLACK markiert.

SPAM-Tags im SMTP-Header:
In manchen Fällen werden Emails durch vorgeschaltete Filter vorqualifiziert. Dieses kann schon beim Provider oder durch eigene Server geschehen. In diesem Fall ist dann der Betreff erweitert oder es befindet sich ein spezielles Tag im Code der Originalnachricht.

- **Mail Header Tag:** Tragen sie hier das auszuwertende Tag so ein, wie sie es in der Original-Nachricht finden. Bespiel: **X-Spam-Flag: YES**. Eine Nachricht, die dieses Tag enthält, wird als SPAM klassifiziert. Mehrere Tags können mit einem Semikolon oder einem senkrechten Strich (Pipe Symbol) getrennt angegeben werden.

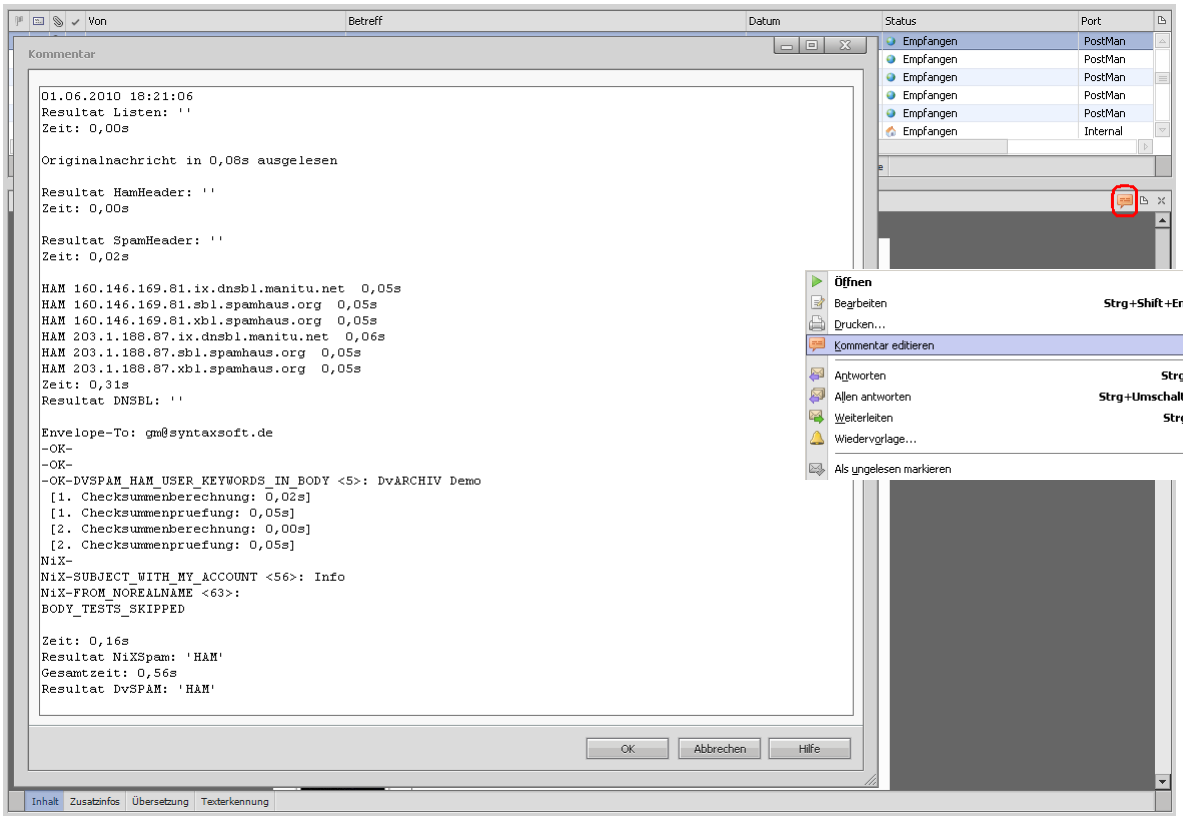
- **Mail Betreff Tag:** Wird dem Betreff ein bestimmtes Tag vorangestellt, können Sie alternativ auch dieses angeben. Bespiel: **[***SPAM**. Eine Nachricht, deren Betreff mit diesem Tag beginnt, wird als SPAM klassifiziert. Mehrere Tags können mit einem Semikolon oder einem senkrechten Strich (Pipe Symbol) getrennt angegeben werden.

HAM-Tags im SMTP-Header:
Z.B. Sie erhalten Kontaktanfragen vom eigenen Webserver bei denen die Kunden Email-Adresse als Absender verwendet wird. Im Code der Originalnachricht befindet sich ein spezielles Tag, der als HAM klassifiziert werden kann.

- **Mail Header Tag:** Tragen sie hier das auszuwertende Tag so ein, wie sie es in der Original-Nachricht finden. Bespiel: „X-Mailer: Mustermann Firma Kontaktformular“. Eine Nachricht, die dieses Tag enthält, wird als HAM klassifiziert. Mehrere Tags können mit einem Semikolon oder einem senkrechten Strich (Pipe Symbol) getrennt angegeben werden.

David Integration :

- **Ergebnis Spam Check in David Kommentar schreiben:** Wird diese Option gewählt, wird das resultierende Ergebnis der Klassifizierung in die Kommentardatei der Nachricht geschrieben und kann dort im David Client eingesehen werden. Den Kommentar einer Nachricht können im Titel der Vorschau oder über das Kontextmenü einer Nachricht öffnen. Mit dieser Funktion ist nach der Konfiguration und dem Start des DvSPAM Service die Überprüfung der korrekten Funktionsweise von DvSPAM möglich.

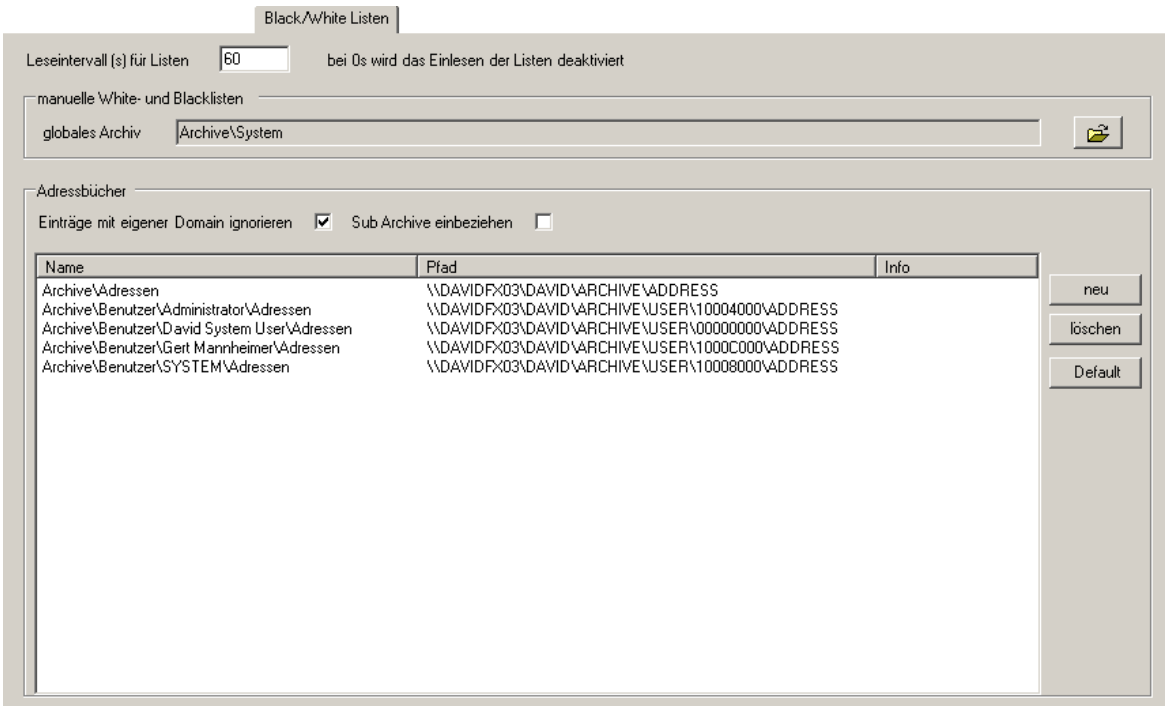


- **Ergebnis Spam Check in Spalte ‚Identifizierung' schreiben:** Wird diese Option gewählt, wird das resultierende Ergebnis der Klassifizierung in die Spalte ‚Identifizierung' der Nachricht geschrieben. Sollten Sie diese Spalte im David Client nicht sehen, können Sie sie über den Dialog ‚Verfügbare Spalten' hinzufügen. Ist diese Option aktiviert, werden neue Nachrichten, die bereits einen Status in dieser Spalte haben, nicht erneut geprüft. Ziehen Sie z.B. eine mit einem Status versehene Nachricht aus dem Spam Archive in den Eingang, wird die Nachricht nicht erneut geprüft.

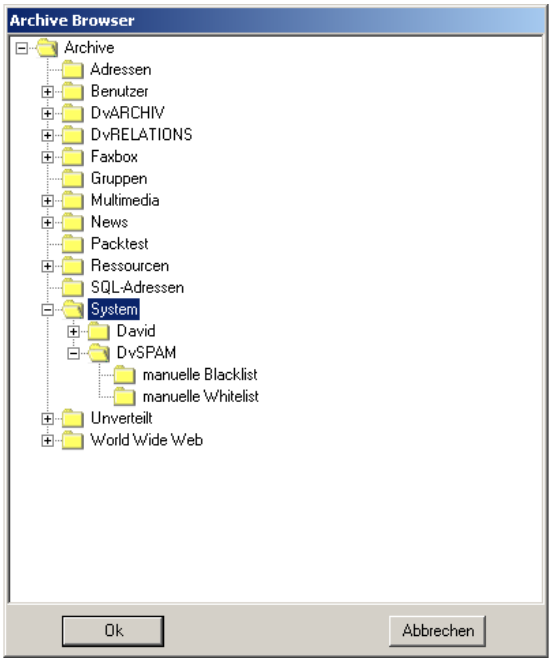
- **Kein Spam Check wenn ein David Kommentar vorhanden ist:** Ist diese Option aktiv, überprüft DvSPAM keine Nachrichten, die bereits einen Kommentar enthalten. Ist diese Option inaktiv und die Option **Ergebnis des Spam Checks in David Kommentar** schreiben aktiv, wird der bereits vorhandene Kommentar überschrieben.

5.3 Registerkarte Black/Whitelisten

Auf dieser Registerkarte werden die manuellen Black- und Whitelisten konfiguriert. Es gibt drei verschiedene Listen: eine Black- und Whiteliste als Archive im David Client. Diese Listen können global von allen Nutzern verwendet werden. Es kann im David Client eine Nachricht in eines dieser beiden Archive kopiert werden. Die Absenderadresse wird daraufhin von DvSPAM pauschal gesperrt oder freigegeben, ohne den Nachrichteninhalt zu untersuchen. Beachten Sie bitte, dass DvSPAM den Nachrichteninhalt, Betreff und Anhänge in diesen Archiven löscht. Alternativ können Sie in beiden Archiven Adressen anlegen oder dorthin kopieren. Von diesen Adressen werden die Emailadressen als Black- oder Whitelisteinträge verwendet. Geben Sie als Mailadresse z.B. nur den Domainnamen an: *@syntaxsoft.de*, dann werden alle Mails dieser Domain gesperrt oder freigegeben. Als dritte Liste können Sie Adress-Archive konfigurieren. Alle Mailadressen aus diesen Adressbüchern werden wie Whitelisteinträge behandelt.



- **Globales Archiv für manuelle White- und Blacklisten**: Vom DvSPAMadministrator werden unterhalb des hier konfigurierten Archives ein Archiv DvSPAM mit 2 Unterarchiven angelegt:



- **Manuelle Blacklist:** Diese Liste kann von den Benutzern manuell gepflegt werden und enthält unerwünschte Absenderadressen. Es ist möglich Nachrichten der unerwünschten Absender in dieses Archiv zu verschieben, zu kopieren oder zu verknüpfen. DvSPAM löscht zur Verringerung des Speicherbedarfs selbstständig alle nicht benötigten Informationen. Es bleibt nur der Absender erhalten. Weiterhin können Adressen direkt in diesem Archiv angelegt oder dorthin verknüpft werden. Jeder Adresseintrag kann unter *email* und *2.email* je eine Adresse für die Blacklist enthalten. Es ist auch möglich, nur die Email-Domäne mit einem vorangestellten @ zu verwenden. In dem Fall werden alle Mails dieser Domain als **BLACK** gekennzeichnet.

- **Manuelle Whitelist:** Diese Liste kann von den Benutzern manuell gepflegt werden und enthält erwünschte Absenderadressen. Es ist möglich Nachrichten der gewünschten Absender in dieses Archiv zu verschieben, zu kopieren oder zu verknüpfen. DvSPAM löscht zur Verringerung des Speicherbedarfs selbstständig alle nicht benötigten Informationen. Es bleibt nur der Absender erhalten. Weiterhin können Adressen direkt in diesem Archiv angelegt oder dorthin verknüpft werden. Jeder Adresseintrag kann unter *email* und *2.email* je eine Adresse für die Whitelist enthalten. Es ist auch möglich, nur die Email-Domäne mit einem vorangestellten @ zu verwenden. In dem Fall werden alle Mails dieser Domain als **WHITE** gekennzeichnet.

Es besteht auch die Möglichkeit, über einen Kontextmenüeintrag im David Client Nachrichten in die Black- bzw. Whitelisten zu übertragen. Dafür ist es notwendig, dass Sie das im Programmverzeichnis mitgelieferte Script **dvspam.vbs** zusammen mit der Symboldatei **dvspam.ico** in der David Benutzerkonfiguration einbinden.

Wenn Sie eine oder mehrere Nachrichten per Kontextmenü in eine Black- oder Whitelist hinzufügen möchten, wird dies über eine Datei im Verzeichnis **David\Clients\DvSPAM** dem DvSPAM Service signalisiert, der wiederum den Kopiervorgang ausführt.

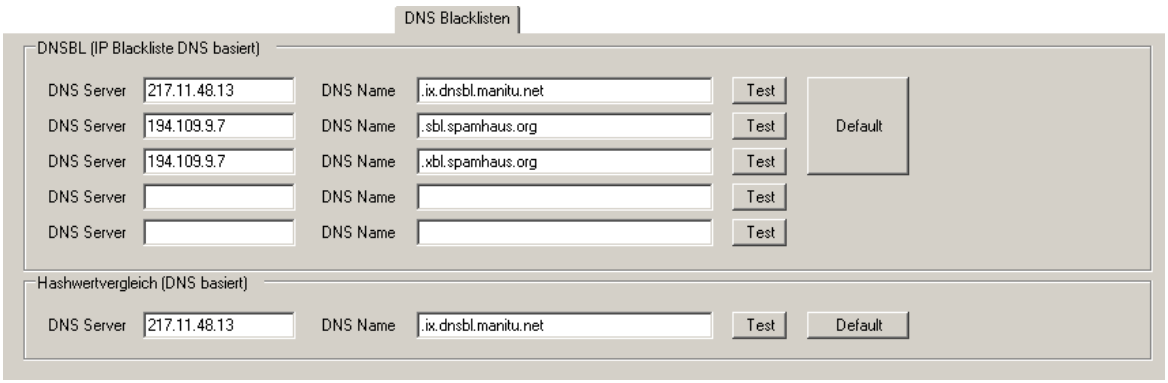
Zusätzlich zu der manuellen und automatischen Whitelist können David Adressbücher als Whitelist verwendet werden. Wählen Sie z.B. das globale und die User Adressbücher aus. Es werden die Mailadressen aller enthaltenen Adresseinträge als Whitelist Einträge behandelt.
Enthalten die Adressbücher Subarchive, können diese bei Auswahl der Option **Sub Archive einbeziehen** eingelesen werden. Enthalten Ihre Adressbücher auch Mailadressen aus Ihren eigenen Domains, würden Mails mit gefälschten Absenderadressen mit Ihren Domains als erwünschte Mail gekennzeichnet werden, da der Absender ja auf der Whitelist enthalten ist. In diesem Fall aktivieren Sie bitte die Option **Einträge mit eigener Domain ignorieren**. Es werden damit alle Adressen, die einen Domainnamen aus der Liste **MY_DOMAIN** enthalten für die Whitelist ignoriert. Der Default Button erzeugt die Einträge für alle Nutzer Adressbücher und das globale Adressbuch.
Beachten Sie bitte, dass es nicht möglich ist SQL Adress-Archive zu verwenden.

5.4 Registerkarte DNS Blacklisten

DvSPAM unterstützt das Onlineabfragen von DNS Blacklisten und Prüfsummen-Listen.

- **DNSBL (IP Blackliste DNS basiert) und Hashwertvergleich (DNS basiert)** Die Daten vom Listenupdate werden vom Heise Verlag auch in einer Listen zur Verfügung gestellt. Der Vorteil einer Onlineabfrage liegt in der Aktualität der Listen. Neu erkannte SPAM Versender werden sofort in die Listen eingetragen. Die dateibasierte Abfrage erhält die neuen Daten i.d.R. deutlich später. Zusätzlich zu der Heise Liste können weitere DNSBL eingetragen werden. Per Default sind bereits zusätzlich zur Heise DNSBL zwei Listen von Spamhaus konfiguriert. Möchten Sie weitere Listen eintragen, benötigen Sie den Domainnamen und die IP Adresse des DNS Server der Liste. Mit dem Testbutton wird eine Testadresse (z.B. 2.0.0.127.ix.dnsbl.manitu.net) bei der Liste angefragt. Diese Adresse ist bei den DNSBL i.d.R. so eingetragen, dass sie als SPAM Versender erscheint. Bei allen Listenantworten mit Adressen aus dem Bereich 127.0.0.X werden die Nachrichten von DvSPAM als SPAM gekennzeichnet.

Für die Onlineabfrage wird eine Freigabe des Ports UDP 53 auf dem Router benötigt.

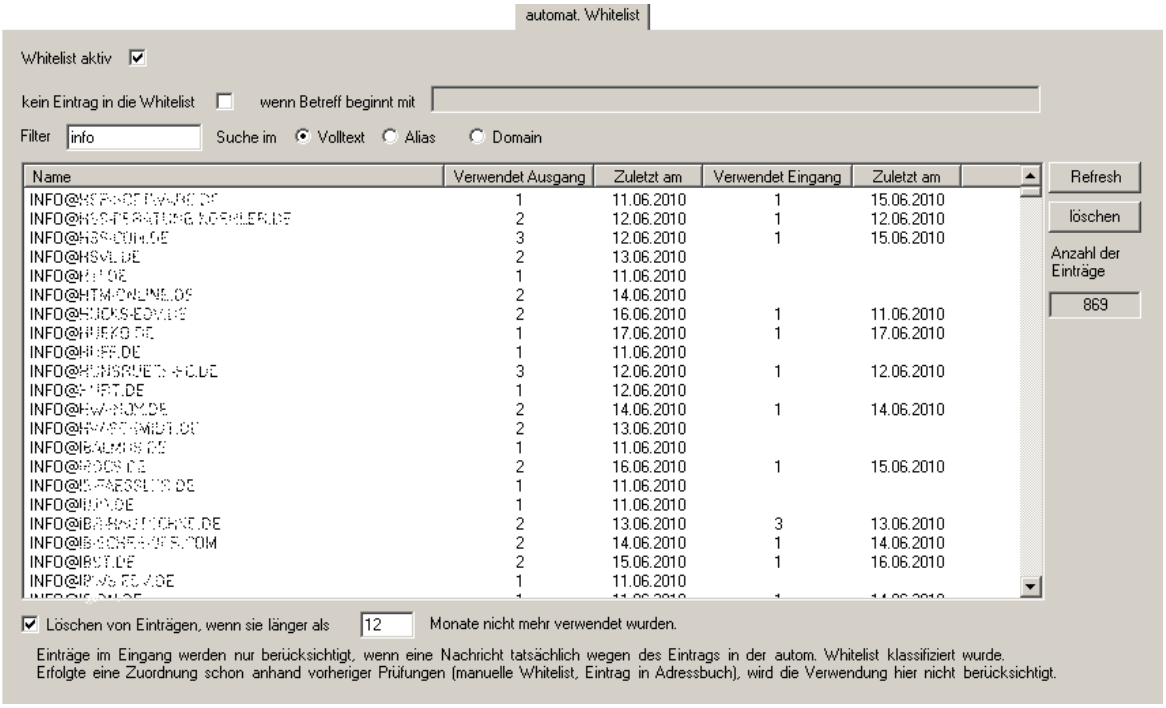


- **DNSBL:** Hier konfigurieren Sie die DNS Blacklisten. Für jede Liste ist die IP Adresse des zugehörigen DNS Servers und die Domainerweiterung notwendig. Mit dem Testbutton kann der Eintrag getestet werden. Dazu wird die Adresse 127.0.0.2 bei der Liste angefragt. I.d.R. ist diese Adresse wie ein SPAM Versender eingetragen. Der Default Button überschreibt die ersten drei Listeneinträge mit den Defaultwerten der NIXSpam und der beiden Spamhaus DNSBL.

- **Hashwertvergleich:** Hier konfigurieren Sie die Liste für den Hashwertvergleich. Für diese Liste ist die IP Adresse des zugehörigen DNS Servers und die Domainerweiterung notwendig. Mit dem Testbutton kann der Eintrag getestet werden. Der Default Button überschreibt den Listeneintrag mit dem Defaultwert des NIXSpam.

5.5 Registerkarte automatische Whitelist

DvSPAM ist selbst lernend. Mails von Absendern, an die Sie Emails senden, sind per Definition keine SPAM-Nachrichten. Interne Mails und Empfänger mit eigener Domain werden nicht in die Liste eingetragen. Sollte der DvSPAM Service laufen und diese Liste erweitern, können Sie sie mit dem Refresh Button neu laden. Möchten Sie Einträge aus dieser Liste entfernen, wählen Sie den oder die Einträge aus und drücken den Löschen-Button oder wählen den entsprechenden Punkt im Kontextmenü aus. Vor dem Ändern beenden Sie bitte den DvSPAM Service.
Damit während der ersten Lernphase Emails Ihrer wichtigen Geschäftspartner nicht als SPAM klassifiziert werden, empfehlen wir Ihnen Ihre Adress-Archive im DvSPAMadministrator zu konfigurieren (s.5.3)



- **Whitelist aktiv**: Mit dieser Option kann die automatische Whitelist aktiviert bzw. deaktiviert werden.

- **Kein Eintrag in die Whitelist**: Wenn Sie diese Option aktivieren, können Sie verhindern, das z.B. AUTOREPLY, Abwesenheitsnotizen oder vergleichbare automatische ausgehende Mails für die automatische Whitelist verwendet werden.

    - **wenn Betreff beginnt mit**: Dafür wird der Beginn des Betreffs der ausgehenden Nachricht mit diesem Datenfeld verglichen. Bei Gleichheit wird der Empfänger der Nachricht nicht auf die automatische Whitelist gesetzt. Verwenden Sie verschiedene automatische Antworten, können Sie diese mit *;* oder | getrennt eintragen.

- **Filter**: Mit dem Filter können Sie die Anzeige der automatischen Whitelist einschränken. Dabei kann die Suche auf den Alias oder die Domain eingeschränkt werden.

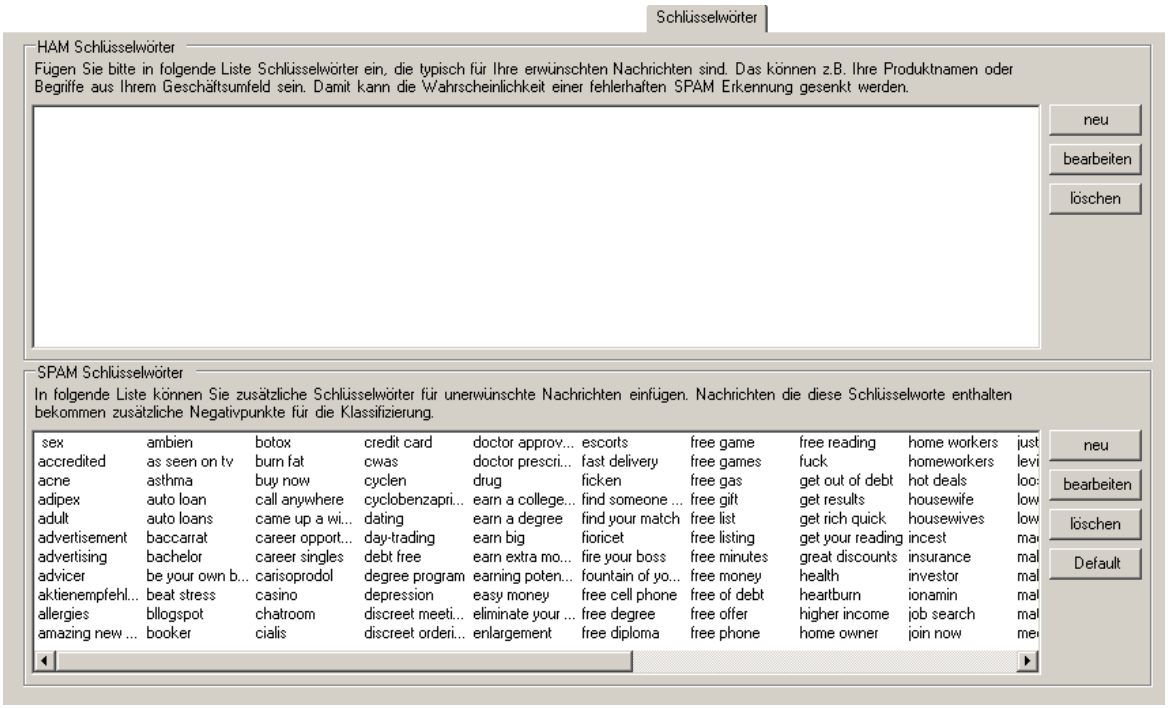
- **Löschen von Einträgen**: Aktivieren Sie diese Option, wenn Einträge aus der automatischen Whiteliste automatisch entfernt werden sollen, wenn Sie innerhalb eines konfigurierbaren Zeitintervalls nicht mehr verwendet wurden.
  Dabei wird berücksichtigt, zu welchem Zeitpunkt an die Adresse zuletzt eine Nachricht verschickt wurde und wann anhand des Eintrags in der automatischen Whiteliste eine Nachricht zuletzt klassifiziert wurde.

5.6 Registerkarte Schlüsselwörter

In der Registerkarte **Schlüsselwörter** können Sie HAM bzw. SPAM Schlüsselwörter eintragen.

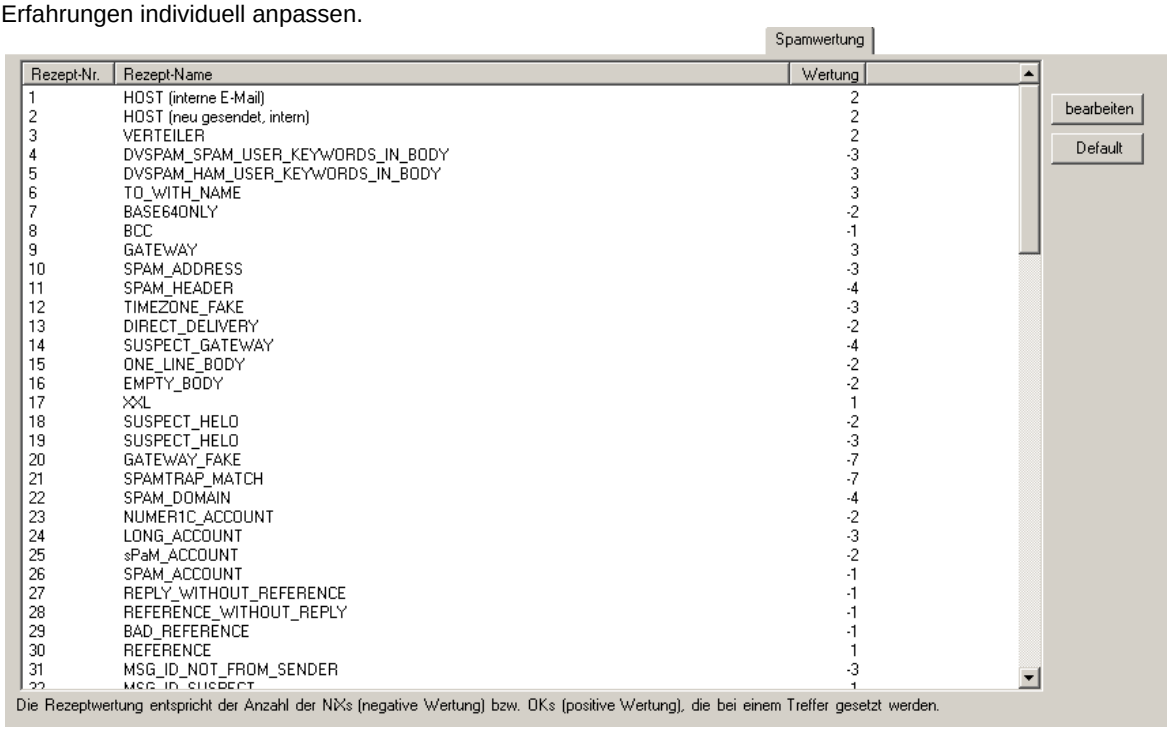
- **HAM Schlüsselwörter:** In diesem Feld können Sie typische Wörter aus Ihrem Geschäftsumfeld eintragen. Enthält eine Nachricht eins dieser Schlüsselwörter, erhält sie bei der Klassifizierung Pluspunkte. Mit dieser Funktion kann die Wahrscheinlichkeit einer falschen Kennzeichnung einer erwünschten Nachricht als SPAM deutlich verringert werden.

- **SPAM Schlüsselwörter:** Enthält eine Nachricht eins dieser Schlüsselwörter, erhält sie bei der Klassifizierung Minuspunkte. Mit dieser Funktion können weitere unerwünschte Nachrichten gefiltert werden.

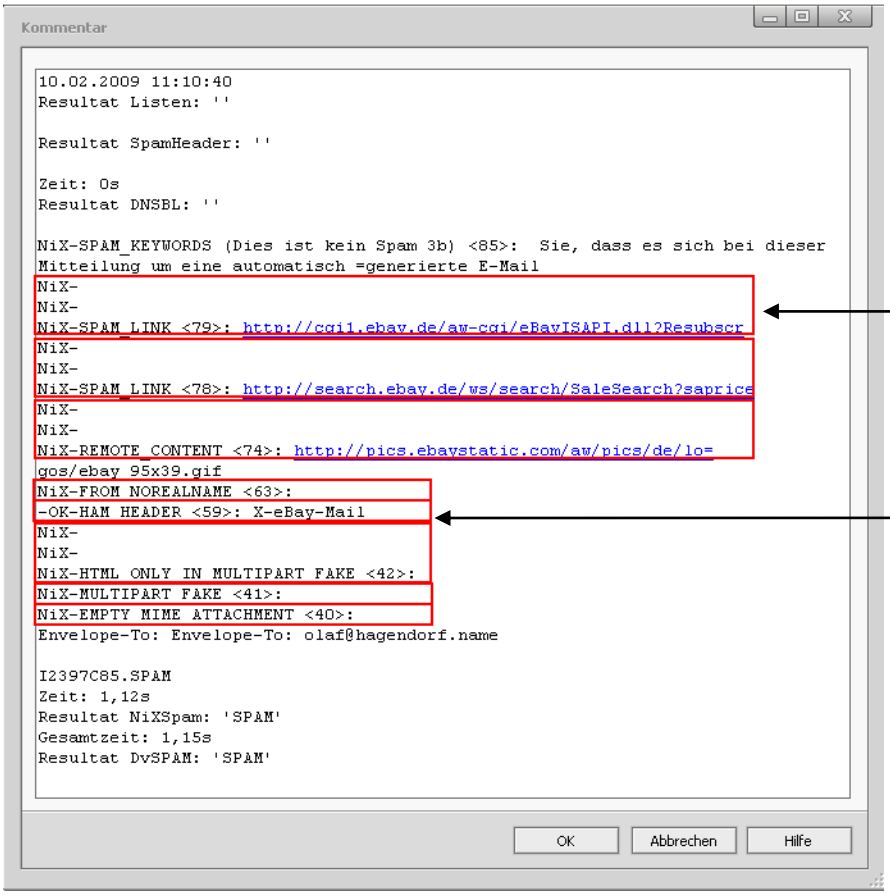

Schlüsselwörter
HAM Schlüsselwörter
Fügen Sie bitte in folgende Liste Schlüsselwörter ein, die typisch für Ihre erwünschten Nachrichten sind. Das können z.B. Ihre Produktnamen oder Begriffe aus Ihrem Geschäftsumfeld sein. Damit kann die Wahrscheinlichkeit einer fehlerhaften SPAM Erkennung gesenkt werden.
neu
bearbeiten
löschen
SPAM Schlüsselwörter
In folgende Liste können Sie zusätzliche Schlüsselwörter für unerwünschte Nachrichten einfügen. Nachrichten die diese Schlüsselworte enthalten bekommen zusätzliche Negativpunkte für die Klassifizierung.
sex ambien botox credit card doctor approv... escorts free game free reading home workers just
accredited as seen on tv burn fat cwas doctor prescri... fast delivery free games fuck homeworkers levi
acne asthma buy now cyclen drug ficken free gas get out of debt hot deals loo
adipex auto loan call anywhere cyclobenzapri... earn a college... find someone ... free gift get results housewife low
adult auto loans came up a wi... dating earn a degree find your match free list get rich quick housewives low
advertisement baccarrat career opport... day-trading earn big fioricet free listing get your reading incest ma
advertising bachelor career singles debt free earn extra mo... fire your boss free minutes great discounts insurance mal
advicer be your own b... carisoprodol degree program earning poten... fountain of yo... free money health investor mal
aktienempfehl... beat stress casino depression easy money free cell phone free of debt heartburn ionamin mal
allergies bllogspot chatroom discreet meeti... eliminate your ... free degree free offer higher income job search mal
amazing new ... booker cialis discreet orderi... enlargement free diploma free phone home owner join now me
neu
bearbeiten
löschen
Default

5.7 Registerkarte Spamwertung

Auf der Registerkarte **Spamwertung** können Sie die Wertigkeit ihrer Nachrichten nach ihren Bedürfnissen und Erfahrungen individuell anpassen.



Angaben zu den angewendeten Rezepten finden Sie, indem Sie sich im David Client von einer Nachricht den Kommentar anzeigen lassen.

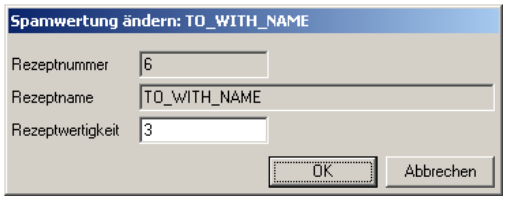


Rezept-Nr. <79>
Rezept-Name SPAM_LINK
Wertigkeit -3 (negative Wertung)

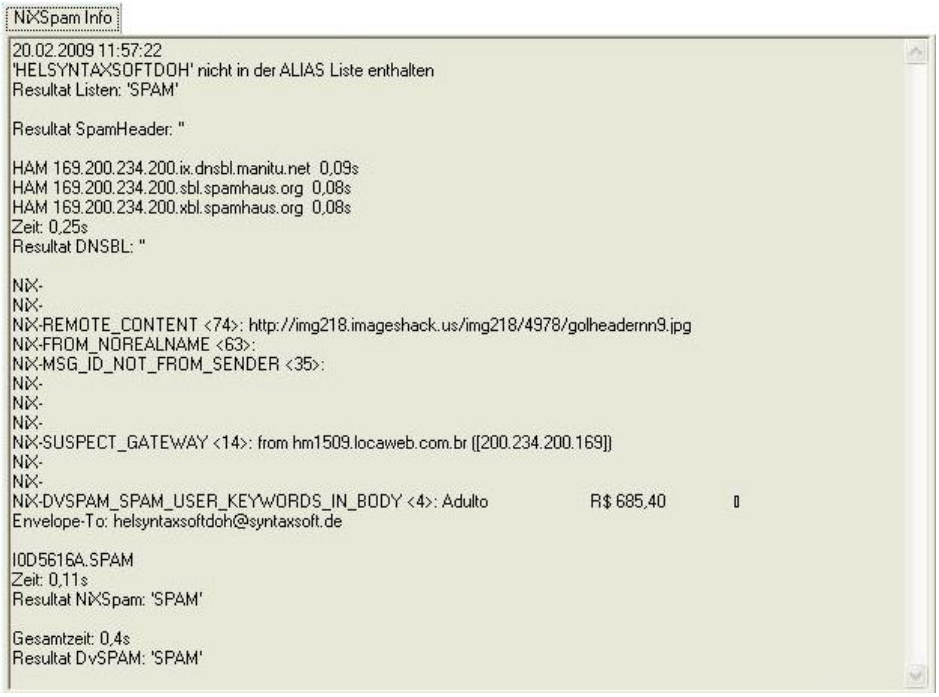
Rezept-Nr. <59>
Rezept-Name HAM_HEADER
Wertigkeit 1 (positive Wertung)

Zum individuellen Anpassen eines Rezeptes:

- Wählen Sie ein Rezept aus und ändern dessen Wertigkeit.



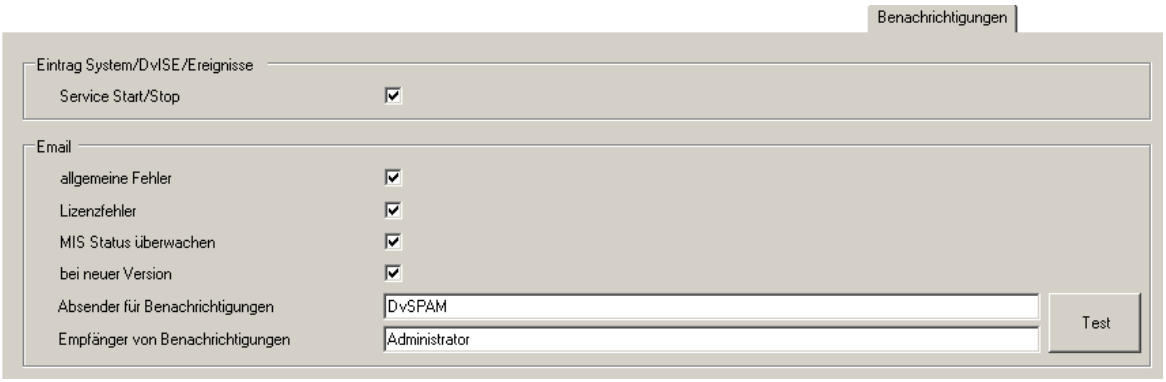
Mit DvSPAMcheck können Sie Ihre geänderten Werte überprüfen. Dazu führen Sie im David Client per Rechtsklick auf eine Nachricht DvSPAMcheck aus.



Ein OK-Punkt besitzt eine höhere Gewichtung als ein NIX-Punkt.

5.8 Registerkarte Benachrichtigungen

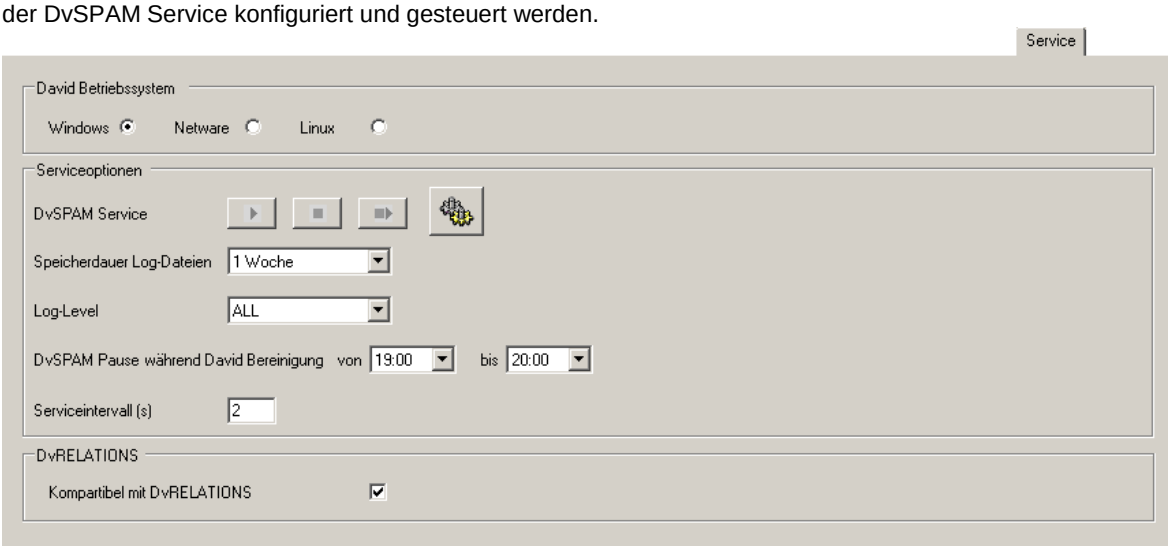
Über die Registerkarte **Benachrichtigungen** kann eine Benachrichtigung bei bestimmten Systemereignissen konfiguriert werden:



- **Allgemeine Fehler, Lizenzfehler:** Aktivieren Sie diese Felder für eine mögliche Fehlerbenachrichtigung
- **MIS Status überwachen:** Aktivieren Sie dieses Feld, für eine Angabe ob der MIS Dienst ein- oder ausgeschaltet ist.
- **Neue Version:** Aktivieren Sie dieses Feld, wenn Sie bei einer neuen verfügbaren Version der Software eine Benachrichtigung erhalten möchten.
- **Absender für Benachrichtigungen**: Tragen Sie hier einen Absender ein, den DvSPAM für den Versand von Benachrichtigungen und Fehlermeldungen verwenden soll. Dies ist im Normalfall eine gültige E-Mail Adresse.
  Beispiel: admin@firma.de
- **Empfänger von Benachrichtigungen:** Tragen Sie hier einen gültigen Empfänger ein, an den DvSPAM Benachrichtigungen und Fehlermeldungen versenden soll. Dies ist im Normalfall eine gültige E-Mail Adresse. Für externe Benutzer ist hierfür natürlich eine funktionsfähige Konfiguration des David Postman erforderlich.
  Beispiel: technik@firma.de
- **Test**: Mit dem Button **Test** können Sie einen Test der Email-Benachrichtigung durchführen:

5.9 Registerkarte Service

Auf der Registerkarte **Service** wird das Betriebssystem auf dem David installiert ist, angezeigt. Weiterhin kann der DvSPAM Service konfiguriert und gesteuert werden.

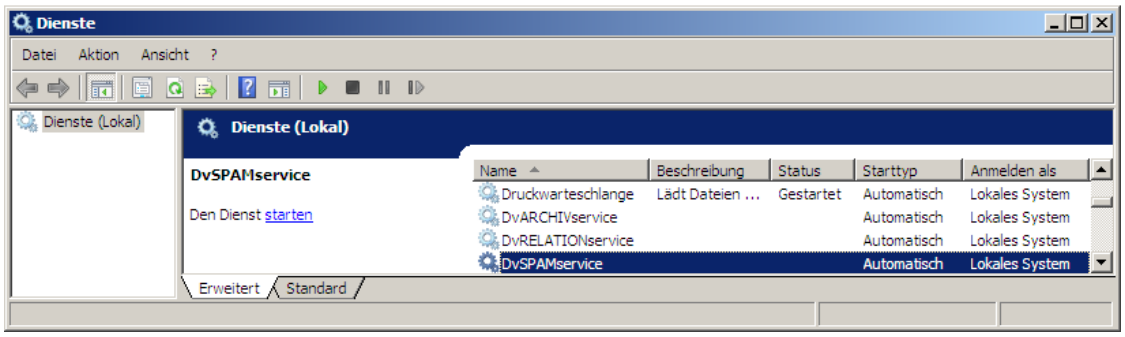


- **David Betriebssystem**: Einige Funktionen von DvSPAM sind betriebssystemspezifisch. Bei der Installation wird das Betriebssystem erkannt. Sollten Sie mit Ihrem David Server umziehen und die Konfiguration von DvSPAM beibehalten, ändern Sie bitte gegebenenfalls diese Konfiguration.

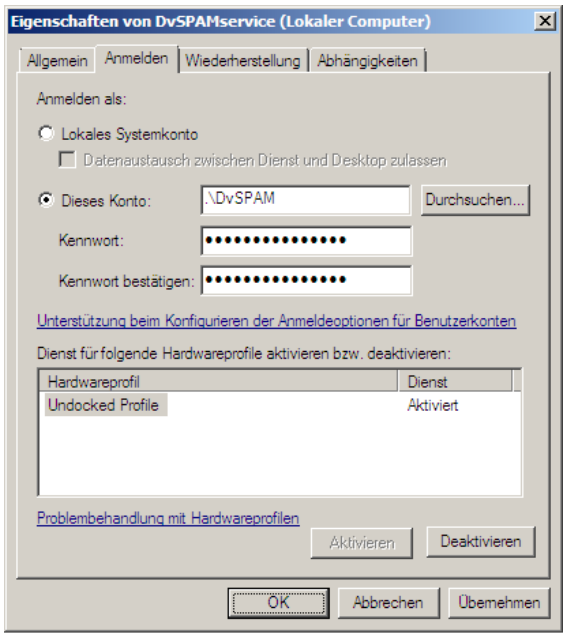
- **DvSPAM Service**: Über die entsprechenden Schaltflächen können Sie die Funktionen **Start**, **Stopp** und **Neustart** des DvSPAM Service ausführen.

Bitte beachten Sie, dass bei deaktivierter Spam-Weiterleitung an Smartphones die Nachrichten aus dem 'In Spamprüfung' Ordner (siehe 5.1) bei gestopptem DvSPAM Service nicht mehr in die Eingangsarchive zurück verschoben werden!

- **Dienste**: Durch Klick auf den Button mit dem Dienste-Symbol rufen Sie den Dialog **Dienste** des Betriebssystems auf:



Wählen Sie den Eintrag **DvSPAM Service** und öffnen sie die Eigenschaften und wechseln Sie bitte zur Registerkarte **Anmelden**:



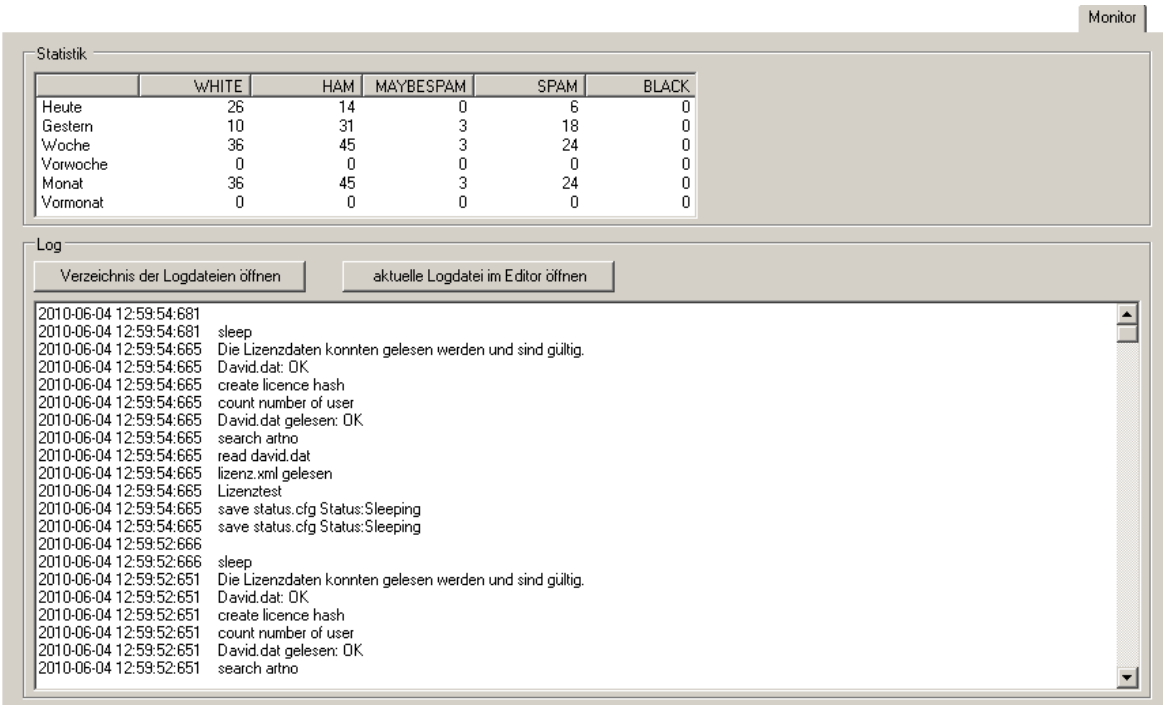
Unter **Anmelden als** wählen Sie bitte die Option **Dieses Konto** aus und tragen den von Ihnen angelegten **DvSPAM Service Account** bzw. den Administrator mit dem zugehörigen Passwort ein. Starten Sie bitte anschließend den DvSPAM Service.

Zur Auswahl der Anmeldung für den DvSPAM Service beachten Sie bitte unbedingt die Hinweise im Kapitel 4.2 - 4.4.

- **Speicherdauer Log-Dateien**: Alle Logdateien die älter sind als der hier eingestellte Wert werden gelöscht.
- **Log-Level**: Das Log-Level definiert die Menge an Informationen, die in die Logdatei geschrieben werden.
  - OFF - es werden keine Ausgaben im Monitor bzw. in der Logdatei vorgenommen
  - ERROR - schreibt Fehler in den Monitor und in die Logdatei
  - WARN - zusätzlich zu ERROR, werden Warnungen ausgegeben
  - INFO - zusätzlich zu WARN, werden normale Ablaufinformationen ausgegeben (empfohlene Defaulteinstellung)
  - ALL - zusätzlich zu INFO, werden detailierte Angaben zum normalen Ablauf ausgegeben
- **Serviceintervall**: Defaulteinstellung - alle 2s wird geprüft, ob neue Nachrichten eingegangen sind, den Wert können Sie nach Ihren Bedürfnissen anpassen
- **Kompartibel mit DvRELATIONS:** Aktivieren Sie diese Option wenn parallel zu DvSPAM auch DvRELATIONS installiert ist. Damit wird dem DvRELATIONS signalisiert, welche Eingangsarchive durch DvSPAM überwacht werden.

5.10 Registerkarte Monitor

Über die Registerkarte **Monitor** kann der DvSPAM Service überwacht werden:


Monitor
Statistik
WHITE HAM MAYBESPAM SPAM BLACK
Heute 26 14 0 6 0
Gestern 10 31 3 18 0
Woche 36 45 3 24 0
Vorwoche 0 0 0 0 0
Monat 36 45 3 24 0
Vormonat 0 0 0 0 0
Log
Verzeichnis der Logdateien öffnen
aktuelle Logdatei im Editor öffnen
2010-06-04 12:59:54:681
2010-06-04 12:59:54:681 sleep
2010-06-04 12:59:54:665 Die Lizenzdaten konnten gelesen werden und sind gültig.
2010-06-04 12:59:54:665 David.dat: OK
2010-06-04 12:59:54:665 create licence hash
2010-06-04 12:59:54:665 count number of user
2010-06-04 12:59:54:665 David.dat gelesen: OK
2010-06-04 12:59:54:665 search artno
2010-06-04 12:59:54:665 read david.dat
2010-06-04 12:59:54:665 lizenz.xml gelesen
2010-06-04 12:59:54:665 Lizenztest
2010-06-04 12:59:54:665 save status.cfg Status:Sleeping
2010-06-04 12:59:54:665 save status.cfg Status:Sleeping
2010-06-04 12:59:52:666
2010-06-04 12:59:52:666 sleep
2010-06-04 12:59:52:651 Die Lizenzdaten konnten gelesen werden und sind gültig.
2010-06-04 12:59:52:651 David.dat: OK
2010-06-04 12:59:52:651 create licence hash
2010-06-04 12:59:52:651 count number of user
2010-06-04 12:59:52:651 David.dat gelesen: OK
2010-06-04 12:59:52:651 search artno

In der Statistik-Anzeige werden die eingegangenen Nachrichten ausgewertet. Sie gibt Auskunft wie viele Nachrichten von heute, gestern, dieser Woche, der letzten Woche, diesen Monats und des Vormonats als WHITE, HAM, MAYBESPAM, SPAM, BLACK erkannt wurden. WHITE und BLACK sind die eingetragenen Adressen in der WHITE- und BLACKLISTE.

Im Log-Anzeigebereich werden die letzten Zeilen der Logdatei dargestellt. Die vollständige Logdatei log.txt liegt im Programmverzeichnis von DvSPAM im Unterverzeichnis **log** (z.B. C:\Programme\DvSPAM\log). Es wird täglich eine neue Logdatei erzeugt. Die alte Datei wird mit dem Tagesdatum als Dateinamen abgelegt.

Die folgenden Funktionen erreichen Sie über das Kontextmenü des Anzeigebereichs. Klicken Sie dazu mit der rechten Maustaste in den weißen Bereich des Monitors:

- **Offline:** Mit dieser Funktion schalten Sie den Monitor offline.
- **Online:** Mit dieser Funktion schalten Sie den Monitor online.
- **Alles markieren:** Markiert den gesamten Inhalt des Anzeigebereiches.
- **Kopieren:** Kopiert den markierten Bereich in die Windows Zwischenablage.

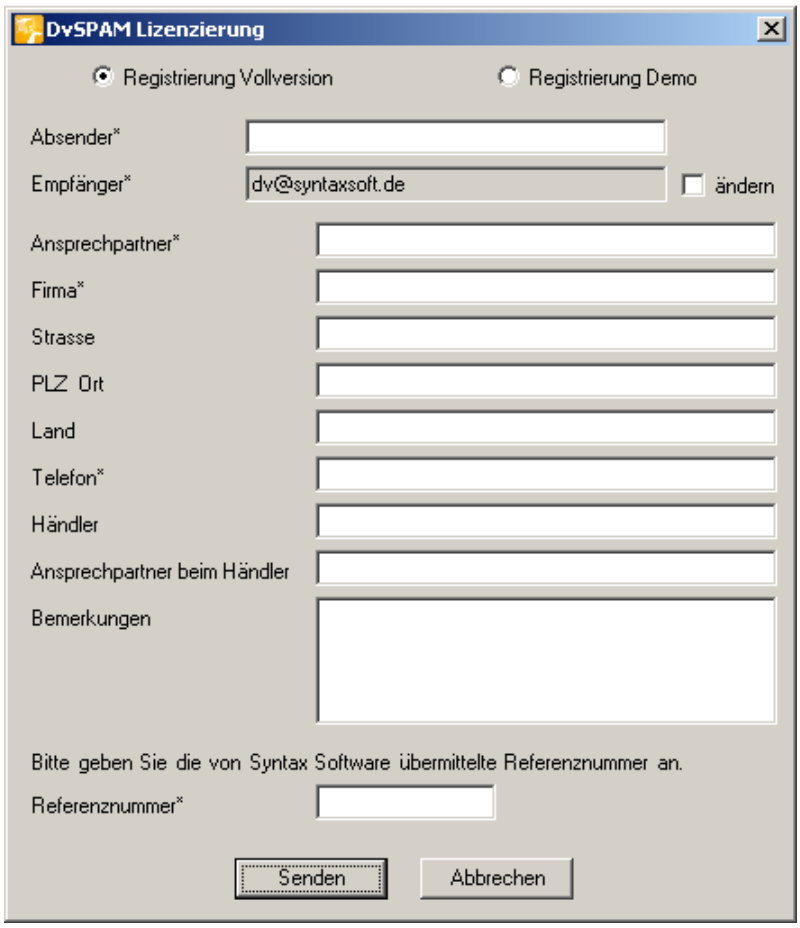
5.11 Info/Lizenzierung Button

Über den Button **Info/Lizenzierung** können Versions- und Lizenzinformationen eingesehen sowie die Lizenzierung durchgeführt werden. Zusätzlich finden Sie hier Links zu www.dv-tools.de und zum DvSPAM Support.

- **Lizenzierung**: Bei nicht gültiger Lizenzierung, beim Betrieb als unlizenzierter Modus oder lizenzierter Demo-Modus steht Ihnen Fenster **Info/Lizenzierung** der Button **Lizenzierung** zur Verfügung.

- **Support-Email erstellen:** Hier senden Sie uns allgemeine Angaben zu Ihrem DvSPAM, wie z.B. die Versions-Nr. und den Systemverwalter. Außerdem befinden sich in der Email Informationen zu den konfigurierten Archiven mit Angabe der Anzahl der Einträge. Im Anhang befinden sich die Lizenz-Datei, das Log und verschiedene Konfigurationsdateien.

Zur Lizenzierung klicken Sie auf den Button **Lizenzierung** und geben die nötigen Informationen ein:



Die Richtigkeit dieser Angaben ist für die Erstellung einer gültigen und lauffähigen Lizenzdatei erforderlich. Sind diese Daten korrekt, wählen Sie bitte **Senden**. Der DvSPAMadministrator übergibt den Sendeauftrag an David. Bitte überprüfen Sie anschließend das Ausgangsarchiv des Administrators auf korrekten Versand.

Bei Ausführung des Lizenzprogramms über den Button **Lizenzierung** sammelt das Lizenzprogramm Informationen über die Tobit Artikelnummern der von Ihnen eingesetzte David-Lizenzen und damit über die Anzahl der am David-Server eingetragenen Benutzerlizenzen. Diese werden per Email zusammen mit den von Ihnen eingetragenen Benutzerinformationen an die SyntaX Software übermittelt. **Weitere Daten** (wie zum Beispiel David Lizenznummern) **werden nicht gewonnen und nicht übermittelt.**

Aus den übermittelten Informationen wird eine Lizenzdatei (lizenz.xml) generiert, welche Ihnen per Email zugesendet wird. Diese Datei ersetzt die Demo- lizenz.xml im DvSPAM Programmverzeichnis. Eine genaue Anleitung finden sie in der Lizenzmail.

Bitte beachten Sie, dass für den Versand der Lizenzdaten per E-Mail eine funktionsfähige Konfiguration des David Postman erforderlich ist.

Sollte es nicht möglich sein, die Lizenzdaten direkt zu versenden, kann die Lizenz auf einem alternativen Weg angefordert werden. Dazu verschicken Sie bitte die beiden Dateien job.txt und Lizenz.txt aus dem DvSPAM Programmverzeichnis an dv@syntaxsoft.de.

5.12 Linux-spezifische Konfiguration

Korrektur der Rechte auf dem David-Linux Server:

Das Archiv DvSPAM (globales Archive für manuelle Black- und Whitelisten, siehe 0) wurde im Linux - Verzeichnis unter dem Namen und mit den Rechten des Windows-Benutzers eingerichtet, unter dem der DvSPAMadministrator läuft. Dies muss korrigiert werden, damit der Benutzer „dvspam“ auf das Verzeichnis zugreifen kann.

Als Beispiel: Sie sind auf der Windows Workstation als Benutzer MEIER angemeldet, haben eine gültige SAMBA-Verbindung zu Ihrem David-Linux Server und installieren DvSPAM. Wenn Sie nun das globale Archiv im David Client festlegen, wird unter Linux das Verzeichnis mit den Rechten und der Eigentümerschaft des Windowsbenutzers angelegt, also z.B. *DvSPAM drwxrwxr-- MEIER:root* Diese Einstellung ist falsch, da dem Benutzer „dvspam“ keine ausreichenden Rechte auf dieses Verzeichnis zur Verfügung stehen. Also muss VOR dem 1. Start des DvSPAM Service korrigiert werden:

- chmod -R 775 DvSPAM
- chown -R root:root DvSPAM

6 Anhang

6.1 Support / Kontakt

Support für DvSPAM erhalten Sie über die DvSPAM Webseite. Hier bieten wir News, FAQs und Informationen rund um DvSPAM. Zusätzlich erreichen Sie SyntaX Software telefonisch oder per E-Mail unter folgenden Adressen:

Downloads:
Download von DvSPAM und aktualisierten Versionen dieses Handbuchs.

Internet:	www.dv-tools.de

Support:

Internet:	www.dv-tools.de
E-Mail:	dv@syntaxsoft.de
Telefon:	03841 / 22 38 - 33

Registrierung:

E-Mail:	dv@syntaxsoft.de

SyntaX Software
Inh. Jörn Satow
Schweinsbrücke 9
23966 Wismar
www.syntaxsoft.de